Cal - H02704 - 73 P014919

(73)

AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY

AND

THE AMERICAN MATHEMATICAL SOCIETY

VOLUME LXXXI

1959

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

P14919

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

INDEX

EIGENFUNCTION EXPANSIONS FOR NON-SYMMETRIC PARTIAL DIFFERENTIAL OPERATORS, II.*

By FELIX E. BROWDER.[1]

Introduction. In a preceding paper [7], we have established an eigenfunction expansion theorem of the Weyl-Plancherel type for any pair of partial differential operators L and B having a realization A which is a subnormal operator in the Hilbert space H_B defined by the positive operator B.[2] It is the purpose of the present paper to extend this result to a much more general class of pairs (L, B) by interpreting the notion of eigenfunction expansion in a more general sense. The class of realization operators for which our results are valid include a significantly large subclass of the unbounded spectral operators in the sense of Dunford ([1], [9]). In addition, the proofs of the expansion theorems of the present paper, which are of a different type than those of [7], enable us to overcome the technical difficulties which arose in [7] as to the nature of the eigenfunctions obtained when the order of B is different from zero.

Let us state the results to be obtained in a more precise way. Let L and B be two partial differential operators defined on an open set G of the n-dimensional Euclidean space E^n, L' the adjoint differential operator of L, $C_c^\infty(G)$ the family of infinitely differentiable functions with compact support in G, and (u, v) the inner product in $L^2(G)$.

We suppose that B is positive, i. e. that $(Bu, u) > 0$ for each u in $C_c^\infty(G)$, and that the Hilbert space H_B with inner product $[\ ,\ ]$ obtained by completing $C_c^\infty(G)$ with respect to the norm $\| u \|_B = (Bu, u)^{\frac{1}{2}}$, has a continuous imbedding in the space of distributions on G. The minimal realization of the pair (L, B) in H_B is the operator A_0 in H_B with domain $C_c^\infty(G)$ defined uniquely by the condition $[A_0 u, v] = (Lu, v), u, v \in C_c^\infty(G)$.

If, by a similar definition, the operator A'_0 in H_B is the minimal realization of the pair (L', B) in H_B, we define the maximal realization of (L, B)

* Received April 1, 1958.

[1] This paper was written while the writer held a National Science Foundation Senior Post-Doctoral Fellowship.

[2] A summary of recent literature on the general theory of eigenfunction expansions for partial differential operators (including [2], [3], [4], [5], [10], [11], [12], [13], [14], and [18]) is given in the Introduction to [7].

to be $A_1 = (A'_0)^*$. More generally, an operator A in H_B will be said to be a realization of the pair (L, B) if $A_0 \subseteq A \subseteq A_1$.

A distribution u on G is said to be an eigenfunction of order one of the pair (L, B) with eigenvalue ζ (ζ a complex number) if $(L - \zeta B)u = 0$. For $k > 1$, by recursion, we define u to be an eigenfunction of order k of the pair (L, B) with eigenvalue ζ if $(L - \zeta B)u = Bv$, where v is an eigenfunction of order $(k-1)$ of (L, B) with eigenvalue ζ. (In an intuitive sense, eigenfunctions of order k correspond to generalized solutions of the equation $(A_1 - \zeta I)^k u = 0$.)

Let C^1 be the set of complex numbers, Ω the σ-algebra of Borel subsets of C^1. In terms of the generalized definition of eigenfunction, the notion of eigenfunction expansion can be described precisely as follows:

Definition 1. An eigenfunction expansion for (L, B) consists of a finite measure m on Ω and two double sequences $\{e_{jk}\}$ and $\{f_{jk}\}$ of functions from C^1 to the space of distributions on G such that:

(a) For all j, k, and ζ, $e_{jk}(\zeta)$ is an eigenfunction of order k of the pair (L, B) with eigenvalue ζ.

(b) For each u in $C_c^\infty(G)$, the function $c_{jk}(\zeta) = (Bu, f_{jk}(\zeta))$ lies in $L^2(m)$, and the mapping U_{jk} defined by $U_{jk}(u) = c_{jk}$ can be extended by continuity to a bounded linear mapping of H_B into $L^2(m)$.

(c) For each c in $L^2(m)$, the integral $\int_{C^1} e_{jk}(\zeta)c(\zeta)\,dm(\zeta)$ converges in the distribution topology to an element h_{jk} of H_B, and the mapping V_{jk} of $L^2(m)$ into H_B defined by $V_{jk}c = h_{jk}$ is a bounded linear mapping.

(d) For each u in H_B, $u = \sum_{j,k} V_{jk} U_{jk} u$.

We remark, writing property (d) out formally, that

$$u(x) = \sum_{j,k} \int_{C^1} e_{jk}(\zeta)\, c_{jk}(\zeta)\, dm(\zeta),$$

justifying the terminology of 'eigenfunction expansion.'

Definition 2. The eigenfunction expansion of Definition 1 is said to be regular if, for each ζ in C^1, $f_{jk}(\zeta)$ is an eigenfunction of the pair (L', B) with eigenvalue $\bar{\zeta}$.

Definition 3. The eigenfunction expansion of Definition 1 is said to be normal if $e_{jk}(\zeta) = f_{jk}(\zeta)$ for all j, k, and ζ, while $V_{jk} = U_{jk}^*$.

We shall prove in Section 4 that an eigenfunction expansion in the sense

of Definition 1 exists for each pair (L, B) having a realization A which belongs to the class of decomposable operators defined below, a regular expansion if A is decomposable of finite order, and a normal expansion if A has a normal decomposition.

The operator A is decomposable if it possesses a decomposition, which, roughly speaking, is a certain infinite-dimensional analogue of the triangular form for finite matrices.[3] More precisely, a decomposition for A consists of the following: a finite measure m on Ω, a bounded linear mapping U of H_B into $L = \sum_{j,k} \oplus (L^2(m))_{jk}$, a bounded linear mapping V of L into H_B, and two bounded linear transformations F and G of L of the form

$$F(\{\alpha_{rs}\})_{jk} = \sum_{s>k} \sum_r f_{jkrs}\alpha_{rs},$$

$$G(\{\alpha_{rs}\})_{jk} = \sum_{s>k} \sum_r g_{rsjk}\alpha_{rs},$$

such that:

(a) $VU = I$.

(b) $U(Au) = M_\zeta Uu + FUu, \ u \in C_c^\infty(G)$ (M_ζ is the multiplication operator by ζ in each component of L).

(c)′ For $\{\alpha_{jk}\}$ in $L^2(m)$ with uniformly bounded support, $\{\alpha_{jk}\} \in L$, $V\{\alpha_{jk}\}$ lies in $D(A)$, and

$$AV(\{\alpha_{rs}\}) = VM_\zeta(\{\alpha_{rs}\}) + VG(\{\alpha_{rs}\}).$$

The decomposition is of order less than k_0 if $U_{jk} = V_{jk} = 0$ for $k \geqq k_0$, and normal if $V = U^*$.

Every operator of the form $A = S + N$, where S is an unbounded scalar operator in the sense of Dunford and N is nilpotent and commutes with the spectral measure of S, is decomposable of finite order. If $A = S + N$, with S a scalar operator, N commuting with the spectral measure of S, and $N^{j(u)}u = 0$ for u in a dense subset of H_B, then A is decomposable.

A is said to be weakly normally decomposable if only (a) and (b) hold while $V_{jk} = U_{jk}^*$. Every restriction of a normally decomposable operator is weakly normally decomposable, so that, in particular, subnormal operators fall in this class. For weakly normally decomposable operators of finite order, we also obtain an eigenfunction expansion theorem.

For subnormal operators, our present results are a sharpening of those of [7] since all the eigenfunctions obtained are distributions rather than

[3] This analogue of the triangular form has very little in common with the generalized triangular form constructed by Lifschitz [15] for operators whose imaginary part has a finite trace.

linear functionals of a more general type. The improvement is brought about by replacing the Banach space differentiation theorem of Birkhoff-Gelfand used in [7] by a result established below on the representation of general linear transformations from an L^p space into the space of distributions of G. For hypoelliptic pairs (L, B), i.e. those for which the distribution solutions of $(L - \zeta B)u = 0$ are differentiable functions for every ζ, we obtain as a result an eigenfunction expansion theorem with smooth eigenfunctions.

Section 1 is devoted to the theory of decomposable and weakly decomposable operators in a separable Hilbert space. Section 2 discusses the functional properties of the space H_B. Section 3 gives the proof of the representation theorem for continuous linear mappings of $L^p(m)$ into $\mathcal{D}'(G)$. Section 4 contains the proof of the expansion theorems for decomposable and weakly decomposable operators. Section 5 gives the application of the expansion theorem to hypoelliptic pairs.

1. Let H be a separable Hilbert space with inner product $[u, v]$, S_0 a dense subset of H. Let T be a linear operator in H with domain $D(T)$ dense in H and range $R(T)$. We suppose that T^*, the adjoint of T, is densely defined in H and that $S_0 \subset D(T) \cap D(T^*)$.

Definition 1.1. Let m be a finite measure on Ω, $\{f_{jkrs}\}$ and $\{g_{jkrs}\}$ two quadruple sequences of m-essentially bounded functions on C^1. Suppose further we are given $\{U_{jk}\}$ a double sequence of bounded linear mappings of H into $L^2(m)$, $\{V_{jk}\}$ a double sequence of bounded linear mappings of $L^2(m)$ into H. Let $L = \sum_{j,k} \oplus (L^2(m))_{jk}$. If $\{\alpha_{rs}\}$ is an element of L, we define the mappings F and G of L into itself by

$$F(\{\alpha_{rs}\})_{jk} = \sum_{s>k} \sum_r f_{jkrs} \alpha_{rs},$$

$$G(\{\alpha_{rs}\})_{jk} = \sum_{s>k} \sum_r g_{rsjk} \alpha_{rs}.$$

In addition, the mappings U of H into L, V of L into H are defined formally by

$$(Uu)_{jk} = U_{jk} u, \qquad V(\{\alpha_{jk}\}) = \sum_{jk} V_{jk}(\alpha_{jk}).$$

The family $(m, \{f_{jkrs}\}, \{g_{jkrs}\}, \{U_{jk}\}, \{V_{jk}\})$ is said to be a permissible system if the mappings F, G, U, and V defined above are all bounded linear mappings.

Definition 1.2. The permissible system $(m, \{f_{jkrs}\}, \{g_{jkrs}\}, \{U_{jk}\}, \{V_{jk}\})$ is said to define a decomposition for the operator T in H with respect to the subset S_0 of H if:

(a) For every u in H, $u=\sum_{jk} V_{jk}U_{jk}u$.

(b) For u in S_0 and ζ in the complement of an m-null set,

$$U_{jk}(Tu)(\zeta)=\zeta U_{jk}(u)(\zeta)+\sum_{s>k}\sum_r f_{jkrs}(\zeta)U_{rs}(u)(\zeta).$$

(c) For u in S_0, α in $L^2(m)$ with bounded support in C^1,

$$[V_{jk}(\alpha),T^*u]=[V_{jk}(\zeta\alpha),u]+\sum_{s>k}\sum_r[V_{rs}(g_{jkrs}\alpha),u].$$

We note that the sum in the last term in the right-hand side of (b) is precisely $(FUu)_{jk}$ as defined in Definition (1.1) and is, therefore, a well-defined element of $L^2(m)$. Similarly, the sum which is the last term in the right-hand side of (c) is equal to $[h,u]$, where $h=VGB_{jk}(\alpha)$, B_{jk} being the injection mapping of $L^2(m)$ into the (j,k)-th component of L.

The following property, which we shall have occasion to use in the discussion of this Section, implies property (c) of Definition (1.2) for any subset S_0 of $D(T^*)$:

(c′) For α in $L^2(m)$ with bounded support in C^1, $V_{jk}(\alpha)$ lies in $D(T)$ and

$$TV_{jk}(\alpha)=V_{jk}(\zeta\alpha)+\sum_{s<k}\sum_r V_{rs}(g_{jkrs}\alpha).$$

Definition 1.3. The decomposition of Definition 1.2 is said to be normal if $V_{jk}=U_{jk}^*$.

If a decomposition is normal, the mapping U of H into L as given in Definition (1.1) is an isometric mapping.

THEOREM 1.1. *Let T be an operator in H such that $T=RT_1R^{-1}$, where T_1 has a decomposition with respect to S_0 satisfying* (c′) *and R is a bicontinuous linear mapping of H onto H. Then T has a decomposition with respect to $R(S_0)$ satisfying* (c′).

Proof. Let $(m,\{f_{jkrs}\},\{g_{jkrs}\},\{U^1{}_{jk}\},\{V^1{}_{jk}\})$ be the permissible system defining the decomposition for T_1 with respect to S of the hypothesis. We define $U_{jk}=U^1{}_{jk}R^{-1}$, $V_{jk}=RV^1{}_{jk}$. It follows easily that $(m,\{f_{jkrs}\},\{g_{jkrs}\},\{U_{jk}\},\{V_{jk}\})$ is a permissible system. We shall verify by direct computation that properties (a) and (b) of Definition (1.2) are satisfied for this system with respect to T and $R(S_0)$, as well as property (c′) above.

For (a): $\sum_{jk} V_{jk}U_{jk}u=R(\sum_{jk} V^1{}_{jk}U^1{}_{jk})(R^{-1}u)=RR^{-1}u=u$, for all u in H.

For (b): If $u \in R(S_0)$, then $R^{-1}u \in S_0$, and we have

$$\begin{aligned} U_{jk}(Tu)(\zeta) &= U^1_{jk}R^{-1}(RT_1R^{-1}u)(\zeta) = U^1_{jk}(T_1R^{-1}u)(\zeta) \\ &= \zeta U^1_{jk}(R^{-1}u)(\zeta) + \textstyle\sum_{s>k}\sum_r f_{jkrs}(\zeta)U^1_{rs}(R^{-1}u)(\zeta) \\ &= \zeta U_{jk}(u)(\zeta) + \textstyle\sum_{s>k}\sum_r f_{jkrs}(\zeta)U_{rs}(u)(\zeta). \end{aligned}$$

For (c′): $T(V_{jk}(\alpha)) = RT_1R^{-1}RV^1_{jk}(\alpha) = RT_1V^1_{jk}(\alpha)$

$$= RV^1_{jk}(\zeta\alpha) + \textstyle\sum_{s<k}\sum_r RV^1_{rs}(g_{jkrs}\alpha) = V_{jk}(\zeta\alpha) + \sum_{s<k}\sum_r V_{rs}(g_{jkrs}\alpha).$$

Definition 1.4. The permissible system $(m, \{f_{jkrs}\}, \{U_{jk}\}, \{V_{jk}\})$ is said to define a weak normal decomposition for T with respect to S_0 if (a) and (b) of Definition (1.2) hold while $V_{jk} = U_{jk}^*$.

THEOREM 1.2. *Let T be an operator in the Hilbert space H, which is a closed subspace of the Hilbert space H_1. Suppose that $T \subseteq T_1$, where T_1 is a normally decomposable operator in H_1 with respect to S_1, $S_0 \subset S_1$. Then T is weakly normally decomposable in H with respect to S_0.*

Proof. Let $(m, \{f_{jkrs}\}, \{g_{jkrs}\}, \{U^1_{jk}\}, \{V^1_{jk}\})$ be a permissible system defining a normal decomposition for T_1 in H_1 with respect to S_1. Let U_{jk} be the restriction of U^1_{jk} to H, and $V_{jk} = PV^1_{jk}$, where P is the projection mapping of H_1 on H. We shall verify that $(m, \{f_{jkrs}\}, \{U_{jk}\}, \{V_{jk}\})$, which is obviously a permissible system, defines a weak normal decomposition for T in H with respect to S_0.

For (a): $\sum_{jk} V_{jk}U_{jk}u = P(\sum_{jk} V^1_{jk}U^1_{jk}u) = Pu = u$, for u in H.

For (b): This follows directly from the fact that $T \subseteq T_1$ and that $U_{jk}u = U^1_{jk}u$ for u in H.

To prove $V_{jk} = U_{jk}^*$: We remark by hypothesis, $V^1_{jk} = (U^1_{jk})^*$. Since U_{jk} is the restriction of U^1_{jk} to H, its adjoint is the projection of the adjoint of U^1_{jk} into H.

Following the terminology of the theory of spectral operators ([9], [1]), we shall denote by a spectral measure on H, a function E from Ω to the bounded operators on H such that:

(i) $E(\phi) = 0$ (ϕ the null set), $E(C^1) = I$.

(ii) For all σ_1, σ_2 in Ω,

$$E(\sigma_1 \cap \sigma_2) = E(\sigma_1)E(\sigma_2),$$
$$E(\sigma_1 \cup \sigma_2) = E(\sigma_1) + E(\sigma_2) - E(\sigma_1)E(\sigma_2).$$

(iii) There exists a constant M with $\| E(\sigma) \| \leq M$ for all σ in Ω.

(iv) For each x and y in H, $[E(\sigma)x, y]$ is countably additive on Ω.

The scalar operator S associated with the spectral measure E is defined by

$$[Su, v] = \int \zeta \, d[E_\zeta u, v]$$

for all u in H for which the integral converges for all v in H.

By a theorem due to Mackey [17] and Lorch [16] (a complete exposition of the proof is given in [20]), for each spectral measure E in H, there exists a bicontinuous linear operator R mapping H onto itself such that $R^{-1}E(\sigma)R$ is an orthogonal projection for every σ in Ω. It follows directly that S is closed and densely defined, that $R^{-1}SR$ is a normal operator in H, and that in (iv) above, we may replace weak countable additivity by strong.

The class of scalar operators in a Hilbert space might thus be defined as the smallest class of (possibly) unbounded operators containing the normal operators which, with each S, contains all operators of the form $R^{-1}SR$, for all bicontinuous linear mappings R of H onto H.

Let N be a bounded operator in H. N is said to commute with the spectral measure E if $E(\sigma)N = NE(\sigma)$ for every σ in Ω. N is said to be semi-nilpotent if there is a dense subset D_1 of H such that for u in D_1, there exists an integer $j(u)$ with $N^{j(u)}u = 0$. By a simple category argument, it follows that if $D_1 = H$, then N is actually nilpotent.

The closed operator T is said to be a spectral operator with respect to the spectral measure E provided that: (1) $E(\sigma)u \in D(T)$ for each u in H and every bounded Borel set σ; (2) For each σ in Ω, $E(\sigma)D(T) \subset D(T)$, while $E(\sigma)Tu = TE(\sigma)u$ for u in $D(T)$; (3) The spectrum of the operator T restricted to the space $E(\sigma)H$ is contained in the closure of σ. If T is bounded, Dunford [9] has shown that $T = S + N$, where S is the scalar operator associated with E and N is a generalized nilpotent ($\| N^n \|^{1/n} \to 0$ as $n \to \infty$) which commutes with the spectral measure E. Conversely, each such operator is a spectral operator. If S is unbounded, N a bounded operator commuting with the spectral measure E such that N is a generalized nilpotent on $E(\sigma)H$ for every bounded Borel set σ, Bade [1] has shown that $S + N$ is a spectral operator.

We shall consider operators of the form $S + N$, where S is a scalar operator (possibly unbounded), N a bounded semi-nilpotent operator commuting with the spectral measure E of S. It follows from the result of Bade that if N is nilpotent, our operators are spectral operators.

THEOREM 1.3. *Let S be a scalar operator with respect to the spectral measure E on the separable Hilbert space H, N a semi-nilpotent operator commuting with E. Then $T = S + N$ is a decomposable operator with a*

decomposition satisfying property (c'). *If N is nilpotent, the decomposition is of finite order. If $N = 0$, the decomposition may be taken of first order.*

Proof. For the subset S_0 with respect to which the decomposition is defined, we choose $D(T) \cap D(T^*)$. It follows by the application of Theorem (1.1) that it suffices to consider the case when S is normal, $E(\sigma)$ a family of orthogonal projections forming the spectral family of S in the sense of the classical spectral theorem for normal operators.

Let $H_k = \{u \mid N^k u = 0\}$. H_k is a closed subspace of H for each k, and $D_1 = \bigcup_k H_k$. Since $E(\sigma)N^k u = N^k E(\sigma)u$ for every σ, it follows that $E(\sigma)H_k \subset H_k$. For $g \in H$, let $H(g)$ be the cyclic subspace generated by g with respect to the spectral measure E, i.e. the span in H of the family $\{E(\sigma)g : \sigma \in \Omega\}$. Since H_k is closed, if $g \in H_k$, $H(g) \subset H_k$.

Let $H_k' = H_k \ominus H_{k-1}$. Since $E(\sigma)H_k \subset H_k$ for every k while $E(\sigma)$ is self-adjoint, it follows that $E(\sigma)H_k' \subset H_k'$. Thus if $g \in H_k'$, $H(g) \subset H_k'$. Since H and therefore H_k' are separable Hilbert spaces, we may choose a sequence $\{g_{jk} : j = 1, 2, \cdots\}$ in H_k' such that $H_k' = \sum_j \oplus H(g_{jk})$. We observe that $H = \sum_{j,k} \oplus H(g_{jk})$, since the dense subset D_1 is contained in the right-hand side. We choose the g_{jk} such that $\| g_{jk} \| = 1$.

Let $m_{jk}(\sigma) = [E(\sigma)g_{jk}, g_{jk}]$, $m(\sigma) = \sum_{jk} 2^{-j-k} m_{jk}(\sigma)$. Let ψ_{jk} be the Radon-Nikodym derivative of m_{jk} with respect to m. Let R_{jk} be the isometric mapping of $L^2(m_{jk})$ into $L^2(m)$ defined by $R_{jk}\alpha = \psi^{\frac{1}{2}}\alpha$, K_{jk} the projection of $L^2(m)$ onto the image of $R_{jk} \cdot K_{jk}\alpha = \Xi_{jk}\alpha$, where Ξ_{jk} is the characteristic function of the set where $\psi_{jk} \neq 0$.

Let W_{jk} be the mapping of $L^2(m_{jk})$ into $H(g_{jk})$ defined in the usual sense by

$$W_{jk}\alpha = \int_{C^1} \alpha(\zeta)\, dE_\zeta g_{jk}, \qquad \alpha \in L^2(m_{jk}).$$

Then W_{jk} is a unitary mapping of $L^2(m_{jk})$ onto $H(g_{jk})$, whose inverse we denote by J_{jk}. We denote by P_{jk} the projection mapping of H on $H(g_{jk})$.

We define the mappings U_{jk} of H into $L^2(m)$, V_{jk} of $L^2(m)$ into H by

$$U_{jk}u = R_{jk}J_{jk}P_{jk}u,$$
$$V_{jk}\alpha = W_{jk}R_{jk}^{-1}K_{jk}\alpha.$$

It follows immediately that $V_{jk} = (U_{jk})^*$.

We note that $N(H_k') \subset H_{k-1} = \sum_{s<k} \sum_r \oplus H(g_{rs})$. Thus for each j and k, $Ng_{jk} = \sum_{s<k} \sum_r W_{rs}(h_{jkrs})$, with h_{jkrs} an uniquely defined element of $L^2(m_{jk})$. We define the quadruple sequences $\{f_{jkrs}\}$ and $\{g_{jkrs}\}$ by

$$g_{jkrs} = \Xi_{jk}\psi_{jk}^{-\frac{1}{2}}\psi_{rs}^{\frac{1}{2}}h_{jkrs}, \; f_{jkrs} = g_{rsjk}.$$

We shall have occasion to apply Theorem XXII of [19], p. 86, which asserts that a set H of distributions on G is bounded in the topology of $\mathfrak{D}'(G)$ if and only if for each open subset G_0 with compact closure in G, there exists an integer $r(G_0)$ and a constant $c(G_0) > 0$ such that

$$\| \lambda \|_{(C^{r(G_0)}(G_0))'} \leqq c(G_0), \tag{2.2}$$

for all λ in H. (In particular, each λ in H is of order $r(G_0)$ at most on G_0).

We shall assume throughout the rest of this paper that B is positive, i.e.

$$(Bu, u) > 0, \qquad u \in C_c^\infty(G). \tag{p_0}$$

The complex vector space $C_c^\infty(G)$ with the inner product $[u, v] = (Bu, v)$ is therefore a pre-Hilbert space, and we may complete it to a Hilbert space H_B with inner product $[u, v]$ and norm $\| u \|_B$.

LEMMA 2.1. *There exists a denumerable dense set in the linear topological space* $C_c^\infty(G)$.

Proof. We shall sketch the proof which is elementary in character. Let j be an element from $C_c^\infty(E^n)$ with $\int j(x)\, dx = 1$. Let F_0 be the family of finite linear combinations with rational coefficients of functions of the form $j_{\epsilon,y}(x) = \epsilon^{-n} j(\epsilon^{-1}(x - y))$, where ϵ is a positive rational number, y is a point of G all of whose coordinates are rational, and ϵ is so small that $j_{\epsilon,y}$ lies in $C_c^\infty(G)$. It is easy to see that for each u in $C_c^\infty(G)$, $u(x) = \int j_{\epsilon,y}(x) p(y)\, dy$ converges to zero in $C_c^\infty(G)$ as $\epsilon \to 0$, and that the integral can be approximated in $C_c^\infty(G)$ by its Riemann sums taken over points y_j with rational coordinates and with rational values assumed by the function $u(y)$.

COROLLARY. *H_B is a separable Hilbert space.*

In addition to (p_0), we make the following sharper assumption on the character of the space H_B.

(p_1) The identity mapping of $C_c(G)$ into $\mathfrak{D}'(G)$ can be extended to a continuous injective mapping J of H_B into $\mathfrak{D}'(G)$.

If (p_1) holds, as we shall assume henceforward, H_B can be continuously identified by J with a linear subset of $\mathfrak{D}'(G)$. It follows from the argument of Section 2 of [17] that (p_1) is implied by the following stronger positivity assumption on the differential operator B:

(p_2) There exists a function p in $C^\infty(G)$ such that $(Bu, u) \geqq (pu, u)$ for all u in $C_c^\infty(G)$.

In the eigenfunction expansion theorems of Section 4, we shall assume only that (p_1) holds, but our conclusions may be strengthened somewhat if (p_2) also holds. In the latter case, J is a continuous mapping not only into $\mathfrak{D}'(G)$ but also into $L^2(p)$.

It follows from Theorem XXII of [19], as stated above, since the image of the unit ball in H_B under J is a bounded set in $\mathfrak{D}'(G)$, that for each open subset G_0 with compact closure in G, there exists an integer $r(G_0)$ and a positive constant $c(G_0)$ such that

$$(2.3) \qquad \| Jv \|_{(C^{r(G_0)}(G_0))'} \leqq c(G_0) \| v \|_B$$

for all v in H_B.

In particular, if u is an element of $C_c^\infty(G)$ and G_0 is an open neighborhood of the support of u with compact closure in G, then

$$(2.4) \qquad |(Lu, v)| \leqq c(G_0) \| Lu \|_{C^r(G_0)} \| v \|_B, \qquad r = r(G_0).$$

Thus for u fixed, (Lu, v) is a bounded conjugate-linear functional defined on the dense subset $C_c^\infty(G)$ of H_B. There exists, therefore, an unique element $A_0 u$ of H_B for which

$$(2.5) \qquad [A_0 u, v] = (Lu, v), \qquad v \in C_c^\infty(G).$$

Definition 2.1. The operator A_0 with domain $C_c^\infty(G)$ in H_B is said to be the minimal realization of the pair of differential operators (L, B).

Let L' be the adjoint differential operator to L on G, defined by $L'u = \sum (-1)^{|\alpha|} D^\alpha (\bar{a}_\alpha(x) u)$ for u in $C_c^\infty(G)$. Let A'_0 be the minimal realization in H_B of the pair (L', B).

Definition 2.2. $A_1 = (A'_0)^*$ is said to be the maximal realization of the pair (L, B).

Definition 2.3. The operator A in H_B is said to be a realization of the pair of differential operators (L, B) if $A_0 \subseteq A \subseteq A_1$.

3. This section is devoted to establishing the following representation theorem for the general continuous linear mapping from an L^p space into $\mathfrak{D}'(G)$.

THEOREM 2.1. *Let m be a finite measure on the σ-algebra Ω of Borel sets of C^1, V a continuous linear mapping of $L^p(m)$ $(1 \leqq p < \infty)$ into $\mathfrak{D}'(G)$. Then there exists a bounded weakly measurable function f from C^1 to $\mathfrak{D}'(G)$ such that*

$$(2.6) \qquad (V\alpha, u) = \int_{C^1} (f(\zeta), u) \alpha(\zeta) \, dm(\zeta),$$

for all u in $C_c^\infty(G)$ and all α in $L^p(m)$.

The distribution $f(\zeta)$ may be chosen so that its order on each open subset G_0 with compact closure in G is bounded for all ζ. If V is a bounded linear mapping into $L^2(p)$ with $p \in C^\infty(G)$, f may be chosen of order $(n+2)$ at most on G for every ζ in C^1.

Proof. Without loss of generality, we may restrict ourselves to an open subset G_0 with compact closure in G. Indeed, if $f_1(\zeta)$ and $f_2(\zeta)$ are functions satisfying the conclusion of the theorem for the open sets G_1 and G_2 respectively, (2.6) implies that

$$(2.7) \qquad \int_{C^1} (f_1(\zeta), u)\,\alpha(\zeta)\,dm(\zeta) = \int_{C^1} (f_2(\zeta), u)\,\alpha(\zeta)\,dm(\zeta)$$

for all u in $C_c^\infty(G_1 \cap G_2)$ and all α in $L^p(m)$. It follows that $(f_1(\zeta), u) = (f_2(\zeta), u)$ for ζ outside a m-null set depending on u. If F_0 is the dense denumerable set in $C_c^\infty(G)$ constructed in Lemma (2.1), it suffices for the equality to hold for u in F_0 in order for it to hold for all u in $C_c^\infty(G)$. Thus $(f_1(\zeta), u) = (f_2(\zeta), u)$ for all u in $C_c^\infty(G)$ for ζ in the complement of a fixed null set. Since $f(\zeta)$ may be taken zero on any m-null set without affecting the validity of (2.6), it follows that the distributions $f_1(\zeta)$ and $f_2(\zeta)$ may be taken equal on $G_1 \cap G_2$ for all ζ. In particular, if $G_1 \subset G_2$, $f_1(\zeta)$ and $f_2(\zeta)$ coincide on G_1 for all ζ. Choosing an increasing sequence G_n of open subsets with compact closure in G whose union equals G, we obtain the desired function for G by taking the common value of $f_m(\zeta)$ on G_n for $m > n$.

Let G_0' be an open subset with compact closure in G such that $\bar{G}_0 \subset G_0'$. On G_0', applying Theorem XXII of [19] once more, the image of $L^p(m)$ under V is contained in the subfamily of distributions of order $\leqq r$, and for all α in $L^p(m)$, we have

$$(2.7) \qquad \| V\alpha \|_{(C^r(G_0'))'} \leqq c \, \| \alpha \|_{L^p(m)}.$$

Let R^n be the dual space to E^n, with the pairing $\langle x, \xi \rangle = \sum_j x_j \xi_j$ for x in E^n, ξ in R^n. For $s > n/2$, we define

$$(2.8) \qquad e_s(x) = \int_{R^n} (|\xi|^2 + 1)^{-s} e^{-i\langle x, \xi \rangle} d\xi.$$

The function $e_s(x)$, which is infinitely differentiable for $x \neq 0$, is a fundamental solution for the elliptic differential operator $Q_s = (-\Delta + 1)^s$, where Δ is the Laplace operator ($\Delta = \sum_j D_j^2$). Let $\epsilon > 0$ be smaller than the distance from G_0 to the complement of G_0', and let $q(x)$ be a function from $C_c^\infty(E^n)$ which is equal to 1 for $|x| < \epsilon/2$, and equal to zero for $|x| \geqq \epsilon$.

Let $e_1(x) = q(x)e(x)$, $e_2(x) = e(x) - e_1(x)$, $e_3(x) = Q_s e_2(x)$. Since $e_2(x) = 0$ in a neighborhood of $x = 0$, e_2 and e_3 lie in $C^\infty(E^n)$.

Suppose that λ is a distribution from $(C^r(G_0'))'$. For z in G_0, $e_1(x-z)$ considered as a function of x has its support in G_0'. Suppose that $2s > r + n$. Then differentiating (2.8) under the integral sign, we see that $e(x)$ lies in $C^r(E^n)$, and hence $e_1(x-z)$ considered as a function of x, $e_{1,z}(x)$, lies in $C_c{}^r(G_0')$. Further, $e_{1,z}$ considered as an element of $C_c{}^r(G_0')$ varies continuously with z for z in G_0.

It follows immediately that $h(z) = (\lambda, e_{1,z})$ is a well-defined, uniformly bounded, continuous function of z in G_0. For u in $C_c{}^\infty(G_0)$, we have, moreover,

$$(2.9)\quad (h, Q_s u) = \int_{G_0} (\lambda, e_{1,z}) Q_s u(z)\,dz = (\lambda_x, \int_{G_0} e_1(x-z) Q_s u(z)\,dz)$$
$$= (\lambda, u) - (\lambda_x, \int_{G_0} e_3(x-z) u(z)\,dz).$$

If we set $k(z) = (\lambda_x, e_3(x-z))$, the last term in (2.9) is equal to (k, u). Since $e_3(x-z)$ has its support in G_0' for z in G_0 and is infinitely differentiable, $k(z)$ is an infinitely differentiable function which is uniformly bounded on G_0 with a bound depending on the $(C^r(G_0'))'$-norm of λ.

Let H and K be the bounded linear mappings of $(C^r(G_0'))'$ into $C^0(G_0)$ defined by $H\lambda = k$, $K\lambda = k$, respectively. Then (2.9) can be written using distribution derivatives in the form

$$(2.10)\qquad \lambda = Q_s H\lambda + K\lambda.$$

Let W and Z be the mappings of $L^p(m)$ into $C^0(G_0)$ defined by $W\alpha = HV\alpha$, $Z\alpha = KV\alpha$. By the Dunford-Pettis theorem [8], there exist functions $w(x,\zeta)$, $z(x,\zeta)$ measurable with respect to the product of Lebesgue measure on G_0 and m on C^1 such that

$$(2.11)\qquad (W\alpha)(x) = \int_{C^1} w(x,\zeta)\alpha(\zeta)\,dm(\zeta); \qquad x \in G_0, \alpha \in L^p(m),$$

$$(2.12)\qquad (Z\alpha)(x) = \int_{C^1} z(x,\zeta)\alpha(\zeta)\,dm(\zeta); \qquad x \in G_0, \alpha \in L^p(m),$$

while there exists a constant c_0 such that for all x in G_0,

$$(2.13)\qquad \| w(x,\text{—}) \|_{L^{p'}(m)} \leqq c_0, \qquad \| z(x,\text{—}) \|_{L^{p'}(m)} \leqq c_0.$$

(p' = the conjugate exponent to p).

From (2.12) and the Fubini theorem (using the boundedness of G_0), we see that for ζ in the complement of a set M_0 of m-measure zero, $w(x,\zeta)$

and $z(x,\zeta)$, considered as functions of x with ζ held fixed, yield elements of $L^{p'}(G_0)$ which we designate as $w(\zeta)$ and $z(\zeta)$. For ζ in M_0, we set $w(\zeta)=0$, $z(\zeta)=0$. In terms of these functions from C^1 to $L^{p'}(G_0)$, (2.12) and (2.13) become

$$W\alpha=\int_{C^1} w(\zeta)\alpha(\zeta)\,dm(\zeta); \qquad Z\alpha=\int_{C^1} z(\zeta)\alpha(\zeta)\,dm(\zeta). \tag{2.14}$$

Finally, we see from (2.10) that $V\alpha=Q_sW\alpha+Z\alpha$. By a simple argument on the convergence of integrals of distributions,

$$V\alpha=\int_{C^1}(Q_sw(\zeta)+z(\zeta))\alpha(\zeta)\,dm(\zeta). \tag{2.15}$$

Equation (2.15) is equivalent to (2.6) if we set $f(\zeta)=Q_sw(\zeta)+z(\zeta)$. The distribution $f(\zeta)$ is of order $2s$ at most on G_0. If V is a continuous linear mapping into $L^2(p)$, then s may be chosen equal to $[n/2]+1$ and $f(\zeta)$ is of order $n+2$ at most on G_0.

4. Let A be a realization of the pair (L,B) in the Hilbert space H_B. We note from the definitions of the minimal and maximal realizations that $C_c^\infty(G)\subset D(A)\cap D(A^*)$.

THEOREM 4.1. *For each decomposition of a decomposable realization A of (L,B) in the Hilbert space H_B, there exists an eigenfunction expansion in the sense of Definition 1 of the Introduction. If the decomposition is of finite order, the corresponding eigenfunction expansion is regular. If the decomposition is normal, the corresponding eigenfunction expansion is normal and* $e_{jk}(\zeta)=f_{jk}(\zeta)$.

Proof. Let $(m,\{f_{jkrs}\},\{g_{jkrs}\},\{U_{jk}\},\{V_{jk}\})$ be a permissible family defining a decomposition of A. We recall that by Definition (1.1),

$$L=\textstyle\sum_{jk}\oplus(L^2(m))_{jk},$$

F and G are bounded linear transformations of L defined by

$$F(\{\alpha_{rs}\})_{jk}=\textstyle\sum_{s>k}\sum_r f_{jkrs}\alpha_{rs}, \tag{4.1}$$

$$G(\{\alpha_{rs}\})_{jk}=\textstyle\sum_{s>k}\sum_r g_{jkrs}\alpha_{rs}. \tag{4.2}$$

U is the bounded linear mapping of H_B into L defined by $(Uu)_{jk}=U_{jk}u$, while V is the bounded linear mapping of L into H_B with

$$V(\{\alpha_{rs}\})=\textstyle\sum_{r,s}(\alpha_{rs}). \tag{4.3}$$

Let B_{rs} be the injection mapping of $L^2(m)$ into the (r,s)-th component of L. For each positive integer r, we define $T_r = F^r U$, a bounded linear mapping of H_B into L. If $T_{r,jk} = B_{jk}^* T_r$ is the projection of T_r on its (j,k)-th component, $T_{r,jk}$ is a bounded linear mapping of H_B into $L^2(m)$. Let $T'_{r,jk} = V G^r B_{jk}$, a bounded linear mapping of $L^2(m)$ into H_B.

In terms of the above definitions, properties (b) and (c) of Definition (1.2) become, respectively:

$$U_{jk}(Au)(\zeta) = \zeta U_{jk}(u)(\zeta) + T_{1,jk}(u)(\zeta), \tag{4.4}$$

$$[V_{jk}(\alpha), A^*u] = [V_{jk}(\zeta\alpha), u] + [T'_{1,jk}(\alpha), u], \tag{4.5}$$

for u in $C_c^\infty(G)$, α in $L^2(m)$ with bounded support.

For the same class of α and u, we obtain by applying properties (b) and (c) of Definition (1.2) to $T_{r,jk}$ and $T'_{r,jk}$ themselves,

$$T_{r,jk}(Au)(\zeta) = \zeta T_{r,jk}(u)(\zeta) + T_{r+1,jk}(u)(\zeta), \tag{4.6}$$

$$[T'_{r,jk}(\alpha), A^*u] = [T'_{r,jk}(\zeta\alpha), u] + [T'_{r+1,jk}(\alpha), u]. \tag{4.7}$$

We remark that equations (4.4) and (4.6) hold for ζ in the complement of an m-null set $M(u)$. By Lemma (2.1), however, $M(u)$ may be chosen independent of u, since we may take $M = \bigcup_t M(u_t)$ for a dense denumerable family $\{u_t\}$ in $C_c^\infty(G)$, and for ζ in the complement of M, (4.4) and (4.6) will hold for all u in $C_c^\infty(G)$ by continuity.

For $r \geqq k$, $T'_{r,jk} = 0$. If the decomposition is of finite order r_0 $T_r = 0$ for $r \geqq r_0$.

We now proceed to the application of Theorem (3.1). The continuous linear mappings U_{jk}^*, V_{jk}, $T_{r,jk}^*$, and $T'_{r,jk}$ of $L^2(m)$ into H_B may be considered, by property (p_1) of Section 2, as continuous linear mappings of $L^2(m)$ into $\mathcal{D}'(G)$. Hence there exist functions $f_{jk}(\zeta)$, $e_{jk}(\zeta($, $t'_{r,jk}(\zeta)$ from $C_2{}^1$ to $\mathcal{D}'(G)$, as described in Theorem (3.1), such that for α in $L^2(m)$,

$$U_{jk}^*(\alpha) = \int_{C^1} f_{jk}(\zeta)\alpha(\zeta)\,dm(\zeta), \tag{4.8}$$

$$V_{jk}(\alpha) = \int_{C^1} e_{jk}(\zeta)\bar{\alpha}(\zeta)\,dm(\zeta), \tag{4.9}$$

$$T_{r,jk}^*(\alpha) = \int_{C^1} t_{r,jk}(\zeta)\alpha(\zeta)\,dm(\zeta), \tag{4.10}$$

$$T'_{r,jk}(\alpha) = \int_{C^1} t'_{r,jk}(\zeta)\alpha(\zeta)\,dm(\zeta). \tag{4.11}$$

For u in $C_c^\infty(G)$, α in $L^2(m)$,

$$\int_{C^1} U_{jk}(u)(\zeta)\bar{\alpha}(\zeta)\,dm(\zeta) = [u, U_{jk}^*(\alpha)] = (Bu, \int_{C^1} f_{jk}(\zeta)\bar{\alpha}(\zeta)\,dm(\zeta)$$
$$= \int_{C^1} (Bu, f_{jk}(\zeta))\bar{\alpha}(\zeta)\,dm(\zeta),$$

the equality of the first with the last term in the chain of equations implying that

$$(4.12) \qquad U_{jk}(u)(\zeta) = (Bu, f_{jk}(\zeta))$$

for ζ in the complement of an m-null set M. Similarly, the equations

$$\int_{C^1} U_{jk}(Au)(\zeta)\bar{\alpha}(\zeta)\,dm(\zeta) = [Au, U_{jk}^*(\alpha)] = (Lu, \int_{C^1} f_{jk}(\zeta)\alpha(\zeta)\,dm(\zeta))$$
$$= \int_{C^1} (Lu, f_{jk}(\zeta))\bar{\alpha}(\zeta)\,dm(\zeta)$$

for u in $C_c^\infty(G)$, α in $L^2(m)$, imply that

$$(4.13) \qquad U_{jk}(Au)(\zeta) = (Lu, f_{jk}(\zeta))$$

in the complement of an m-null set. Parallel arguments for $T_{r,jk}$ *yield*

$$(4.14) \qquad T_{r,jk}(u)(\zeta) = (Bu, t_{r,jk}(\zeta)),$$

$$(4.15) \qquad T_{r,jk}(Au)(\zeta) = (Lu, t_{r,jk}(\zeta))$$

for all u in $C_c^\infty(G)$ and ζ in the complement of an m-null set.

The equations (4.4) and (4.6) become, respectively,

$$(4.16) \qquad (Lu, f_{jk}(\zeta)) = \zeta(Bu, f_{jk}(\zeta)) + (Bu, t_{1,jk}(\zeta)),$$

$$(4.17) \qquad (Lu, t_{r,jk}(\zeta)) = \zeta(Bu, t_{r,jk}(\zeta)) + (Bu, t_{r+1,jk}(\zeta)),$$

for all u in $C_c^\infty(G)$ and ζ in the complement of an m-null set M. Since we may alter any of the functions f_{jk}, e_{jk}, $t_{r,jk}$, and $t'_{r,jk}$ on an m-null set without affecting the validity of any of the previous equations, we may set all of them equal to zero on M. Then (4.16) and (4.17) are valid for all ζ in C^1. In terms of distribution derivatives, they may be written as

$$(4.16)' \qquad L'f_{jk}(\zeta) - \bar{\zeta}Bf_{jk}(\zeta) = Bt_{1,jk}(\zeta)$$

$$(4.17)' \qquad L't_{r,jk}(\zeta) - \bar{\zeta}Bt_{r,jk}(\zeta) = Bt_{r+1,jk}(\zeta).$$

If the decomposition is of finite order r_0, we have $t_{r,jk} = 0$ for $r \geqq r_0$, and f_{jk} is an eigenfunction of order r_0 of (L', B) with eigenvalue $\bar{\zeta}$.

Similarly, equations (4.5) and (4.7) written in terms of the functions $e_{jk}(\zeta)$ and $t'_{r,jk}(\zeta)$ become for u in $C_c^\infty(G)$,

$$(4.18)\qquad (e_{jk}(\zeta), L'u) = \zeta(e_{jk}(\zeta), Bu) + (t'_{1,jk}(\zeta), Bu),$$

$$(4.19)\qquad (t'_{r,jk}(\zeta), L'u) = \zeta(t'_{r,jk}(\zeta), Bu) + (t'_{r+1,jk}(\zeta), Bu),$$

which, after a change of the functions e_{jk} and $t'_{r,jk}$ on a m-null set independent of u, are valid for all ζ in C^1. In terms of distribution derivatives, (4.18) and (4.19) may be written as

$$(4.18)'\qquad Le_{jk}(\zeta) - \zeta Be_{jk}(\zeta) = Bt'_{1,jk}(\zeta),$$

$$(4.19)'\qquad Lt'_{r,jk}(\zeta) - \zeta Bt'_{r,jk}(\zeta) = Bt'_{r+1,jk}(\zeta).$$

Since $t'_{r,jk}(\zeta)$ may be chosen null for all ζ in C^1 if $r \geqq k$, it follows that $e_{jk}(\zeta)$ is an eigenfunction of order k of (L, B) with eigenvalue ζ.

Finally, if $V_{jk} = U_{jk}^*$, $e_{jk}(\zeta) = f_{jk}(\zeta)$ for all ζ, and the decomposition is normal.

Thus all of the conclusions of the theorem have been verified, since the functions $\{e_{jk}(\zeta)\}$ and $\{f_{jk}(\zeta)\}$ yield an eigenfunction expansion in the sense of Definition 1 which is regular if the decomposition is of finite order and normal if the decomposition is normal.

THEOREM 4.2. *To each weak normal decomposition of finite order of a realization A of (L, B), there corresponds a finite measure m on Ω and a double sequence $\{f_{jk}(\zeta)\}$ of functions from C^1 to $\mathfrak{D}'(G)$ such that for each u in $C_c^\infty(G)$, $c_{jk}(\zeta) = (Bu, f_{jk}(\zeta))$ lies in $L^2(m)$, the mapping U defined by $U_{jk}u = c_{jk}$ defines an isometry of H_B into L, for each u in H_B,*

$$u = \Sigma_{j,k} \int_{C^1} f_{jk}(\zeta) U_{jk}(u)(\zeta)\, dm(\zeta),$$

while $f_{jk}(\zeta)$ is an eigenfunction of (L', B).

Proof. The present conclusions follow immediately from the portion of the preceding proof that remains valid for a weak normal decomposition.

5. To derive eigenfunction expansions in the classical sense from the theorems of the previous section, we must restrict ourselves to a subclass of pairs (L, B) for which the distribution eigenfunctions are ordinary differentiable functions. The simplest, and the widest such subclass, is of course that covered by the following definition.

Definition 5.1. The pair of differential operators (L, B) is said to be hypoelliptic in the widest sense if every distribution solution u of the equation $(L - \zeta B)u = v$ with v in $C^\infty(G)$, is itself an infinitely differentiable function in G.

It is an immediate consequence of Definition (5.1) that for a pair (L, B) which is hypoelliptic in the widest sense, every eigenfunction of arbitrary order of (L, B), for arbitrary eigenvalue ζ, is an infinitely differentiable function.

To obtain further regularity properties for the eigenfunction expansions obtained in the theorems of Section 4, we introduce the spaces $W^{r,2}(G_0)$ and the (r, G_0)-norm, where G_0 is an open subset of G and r is an integer. For $r \geqq 0$,

$$W^{r,2}(G_0) = \{u : D^\alpha u \in L^2(G_0) \text{ for } |\alpha| \leqq r\}.$$

The corresponding norm is given by $(\| u \|_{r,G_0})^2 = \int_{G_0} \sum_{|\alpha| \leqq r} |D^\alpha u|^2 \, dx$. For $r < 0$, $W^{r,2}(G_0) = \{u : |(u, \psi)| \leqq c(u) \| \psi \|_{r,G_0}, \psi \in C_c^\infty(G_0)\}$. The corresponding norm is given by

$$\| u \|_{r,G_0} = \sup\{|(u, \psi)| : \psi \in C_c^\infty(G_0), \| \psi \|_{-r,G_0} \leqq 1\}.$$

Definition 5.2. The pair of differential operators (L, B) is said to be hypoelliptic in the strong sense if given two open subsets G_0 and G_0' with compact closure in G, $\bar{G}_0 \subseteq G_0'$, and an integer j, there exists a constant $c(G_0, G_0', j) > 0$ such that if u is a distribution solution of the equation $Lu = Bv$ with $\| u \|_{j,G_0'} < \infty$, $\| v \|_{j,G_0'} < \infty$, then

$$\| u \|_{j+1,G_0} \leqq c(G_0, G_0', j)\{\| u \|_{j,G_0'} + \| v \|_{j,G_0'}\} < \infty. \tag{5.1}$$

THEOREM 5.1. *Let (L, B) and (L', B) be pairs of differential operators hypoelliptic in the strong sense on G, A a decomposable realization of (L, B). Then the functions $\{e_{jk}(\zeta)\}$ and $\{f_{jk}(\zeta)\}$ obtained in Theorem (4.1) may be chosen infinitely differentiable for all ζ in C^1. Further, for every open subset G_0 with compact closure in G, bounded Borel set σ in C^1, and positive integers r and k, there exists a positive constant $c(G_0, \sigma, r, k)$ such that*

$$\begin{aligned} &\int_\sigma |D^\alpha e_{jk}(x, \zeta)|^2 \, dm(\zeta) \leqq c(G_0, \sigma, r, k), \\ &\int_\sigma |D^\alpha f_{jk}(x, \zeta)|^2 \, dm(\zeta) \leqq c(G_0, \sigma, r, k) \end{aligned} \tag{5.2}$$

for all x in G_0, $|\alpha| \leqq r$.

Proof. It follows from the proof of Theorem (3.1) that there exists a positive integer s, depending only on G_0 and on the imbedding of H_B in $\mathfrak{D}'(G)$, and sequences of functions $\{p_{jk}(x,\zeta)\}$, $\{q_{jk}(x,\zeta)\}$, $\{p_{r,jk}(x,\zeta)\}$, $\{q_{r,jk}(x,\zeta)\}$ such that

$$\begin{aligned} e_{jk}(x,\zeta) &= (-\Delta+1)^s p_{jk}(x,\zeta), \\ f_{jk}(x,\zeta) &= (-\Delta+1)^s q_{jk}(x,\zeta), \\ t'_{r,jk}(x,\zeta) &= (-\Delta+1)^s p_{r,jk}(x,\zeta), \\ t_{r,jk}(x,\zeta) &= (-\Delta+1)^s q_{r,jk}(x,\zeta), \end{aligned} \tag{5.3}$$

while there exists a constant $c(G_0,B)$ such that

$$\begin{aligned} &\int_{C^1} |p_{jk}(x,\zeta)|^2\, dm(\zeta) \leqq c(G_0,B)\, \|V_{jk}\|^2, \\ &\int_{C^1} |q_{jk}(x,\zeta)|^2\, dm(\zeta) \leqq c(G_0,B)\, \|U_{jk}\|^2, \\ &\int_{C^1} |p_{r,jk}(x,\zeta)|^2\, dm(\zeta) \leqq c(G_0,B)\, \|T'_{r,jk}\|^2, \\ &\int_{C^1} |q_{r,jk}(x,\zeta)|^2\, dm(\zeta) \leqq c(G_0,B)\, \|T_{r,jk}\|^2, \end{aligned} \tag{5.4}$$

for all x in G_0. Noting by Definition (1.1) that $\|U_{jk}\|$ and $\|V_{jk}\|$ are uniformly bounded for all j and k, and that $\|T'_{r,jk}\| \leqq c(r)$, $\|T_{r,jk}\| \leqq c(r)$, we obtain from (5.3), (5.4), and the definition of the negative norms given above.

$$\begin{aligned} &\int_{C^1} \|e_{jk}(\zeta)\|^2_{-2s,G_0}\, dm(\zeta) \leqq c_0, \\ &\int_{C^1} \|f_{jk}(\zeta)\|^2_{-2s,G_0}\, dm(\zeta) \leqq c_0, \\ &\int_{C^1} \|t'_{r,jk}(\zeta)\|^2_{-2s,G_0}\, dm(\zeta) \leqq c(r), \\ &\int_{C^1} \|t_{r,jk}(\zeta)\|^2_{-2s,G_0}\, dm(\zeta) \leqq c(r), \end{aligned} \tag{5.5}$$

with the integrands in each of the integrals of (5.5) finite for ζ in the complement of an m-null set. If we set all the various functions equal to zero for ζ in the m-null set concerned, the integrands will be finite for all ζ in C^1. From the proof of Theorem (4.1), we have

$$
(5.6)\qquad
\begin{aligned}
Le_{jk}(\zeta) &= \zeta Be_{jk}(\zeta) + Bt'_{1,jk}(\zeta),\\
Lt'_{r,jk}(\zeta) &= \zeta Bt'_{r,jk}(\zeta) + Bt'_{r+1,jk}(\zeta),\\
L'f_{jk}(\zeta) &= \bar{\zeta} Bf_{jk}(\zeta) + Bt_{1,jk}(\zeta),\\
L't_{r,jk}(\zeta) &= \bar{\zeta} Bt_{r,jk}(\zeta) + Bt_{r+1,jk}(\zeta).
\end{aligned}
$$

It follows from the Definition (5.2) of hypoellipticity in the strong sense, by a simple inductive argument starting from the finiteness of the $(-2s, G_0)$-norms of all the functions concerned, that the (r, G_0'')-norm of each function is finite for all r and every G_0'' with compact closure in G_0. It follows from a well-known theorem of Sobolev ([19], vol. 2) that the functions $e_{jk}(x,\zeta)$ and $f_{jk}(x,\zeta)$ are infinitely differentiable in x in G_0 for every ζ in C^1.

The inequalities (5.2) follow from (5.5), (5.6), and Definition (5.2) by a direct inductive argument.

Remark. Conditions for the hypoellipticity of (L, B) in terms of the characteristic forms of the operators L and B may be obtained from the results of [14] and [6]. If L is elliptic and B is of order less than the order of L, then (L, B) is hypoelliptic in the strong sense. Since every non-degenerate ordinary differential operator is elliptic, the latter class includes all pairs (L, B) treated in the theory for ordinary differential operators.

YALE UNIVERSITY.

REFERENCES.

[1] W. Bade, "Unbounded spectral operators," *Pacific Journal of Mathematics*, vol. 4 (1954), pp. 373-392.

[2] W. Bade and J. T. Schwartz, "On Mautner's' eigenfunction expansions," *Proceedings of the National Academy of Sciences*, vol. 42 (1956), pp. 519-525.

[3] Yu. M. Berezanski, "On expansion in eigenfunctions of general self-adjoint differential operators," *Doklady Akademii Nauk* (N.S.), vol. 108 (1956), pp. 379-382.

[4] F. E. Browder, "Eigenfunction expansions for singular elliptic operators, I and II," *Proceedings of the National Academy of Sciences*, vol. 40 (1954), pp. 454-463.

[5] ———, "Eigenfunction expansions for formally self-adjoint partial differential operators, I and II," *ibid.*, vol. 42 (1956), pp. 769-771, 870-872.

[6] ———, "Regularity theorems for solutions of partial differential equations with variable coefficients," *ibid.*, vol. 43 (1957), pp. 234-236.

n16719

[7] ———, "Eigenfunction expansions for non-symmetric partial differential operators, I," *American Journal of Mathematics*, vol. 80 (1958), pp. 365-381.

[8] N. Dunford and B. J. Pettis, "Linear operations on summable functions," *Transactions of the American Mathematical Society*, vol. 47 (1940), pp. 323-392.

[9] N. Dunford, "Spectral operators," *Pacific Journal of Mathematics*, vol. 4 (1954), pp. 321-354.

[10] L. Garding, "Eigenfunction expansions connected with elliptic differential operators," *Proceedings of the 12th Congress of Scandinavian Mathematicians*, Lund, 1954.

[11] ———, "Applications of the theory of direct integrals of Hilbert spaces to some integral and differential operators," *Lecture Series No. 11*, Institute for Fluid Dynamics and Applied Mathematics, University of Maryland, 1954.

[12] I. M. Gelfand and A. G. Kostyucenko, "On expansions in characteristic functions of differential operators and other operators," *Doklady Akademii Nauk* (N. S), vol. 103 (1955), pp. 349-352.

[13] I. M. Gelfand and G. E. Silov, "Quelques applications de la theorie des fonctions generalisées," *Journal de Mathématiques Pures et Appliquées*, vol. 35 (1956), pp. 383-413.

[14] L. Hormander, "On the theory of general partial differential operators," *Acta Mathematica*, vol. 94 (1955), pp. 161-248.

[15] M. S. Lifschitz, "On the spectral decomposition of linear non-self-adjoint operators," *Matematičeskiĭ Sbornik* (N. S), vol. 34 (1954), pp. 145-199. (American Mathematical Society Translation Series 2, vol. 5.)

[16] E. R. Lorch, "The spectrum of linear transformations," *Transactions of the American Mathematical Society*, vol. 52 (1942), pp. 238-248.

[17] G. W. Mackey, *Commutative Banach Algebras*, multigraphed Harvard notes, 1952.

[18] F. I. Mautner, "On eigenfunction expansions," *Proceedings of the National Academy of Sciences*, vol. 39 (1953), pp. 49-53.

[19] L. Schwartz, *Theorie des distributions*, Vols. I and II, Paris, 1951.

[20] J. Wermer, "Commuting spectral measures on Hilbert space," *Pacific Journal of Mathematics*, vol. 4 (1954), pp. 355-361.

SINGULAR INTEGRALS IN TWO DIMENSIONS.*

By JOHN J. McKIBBEN.[1]

1. Introduction. We recall that a real-valued C^∞ function $u = (x_1, x_2)$ of the two real variables x_1 and x_2 is said to be "rapidly decreasing" if the absolute value of the function $P(x_1, x_2)Du$ is bounded on R^2 for all real polynomials $P(x_1, x_2)$ and all partial derivatives Du of u. The space of all C^∞ rapidly decreasing function on R^2 is topologized according to the method of Laurent Schwartz [6], and the resulting space will be denoted by (ζ). A "tempered distribution" is a continuous linear mapping of (ζ) into the real numbers.

It is well-known that every function which is locally square integrable is a distribution [6]. On the other hand, as this paper is written, it appears to be unknown whether or not even some of the simplest functions which are not locally square integrable—for example, the reciprocals of polynomials of several variables—are distributions. We prove here that the reciprocal of any polynomial in two real variables is a distribution and that it is, in fact, a tempered distribution. More significant, perhaps, is the fact that the proof we give is entirely constructive and yields a method for computing the reciprocal of any polynomial in two variables. As the author will show in another paper, a variant of the same method allows one to construct the reciprocal of an arbitrary analytic function of two real variables.

It may be useful to express the analytical content of our main result in terms of the more widely known, if somewhat more obscure, idea of a "partie finie" of a divergent integral. Rephrased, the theorem says that if $q(\eta_1, \eta_2)$ is any polynomial in two variables, it is possible to define in the sense of Hadamard the expression

$$Pf. \int_{R^2} u(\eta_1, \eta_2) [q(\eta_1, \eta_2)]^{-1} d\eta_1 d\eta_2.$$

In our proof, we follow Hadamard's procedure of integrating by parts and then discarding the boundary integrals which tend to become infinite.

* Received February 12, 1958.

[1] This research was supported in part by the Office of Ordnance Research under Contract DA-11-022-ORD-1833 and in part by a National Science Foundation Fellowship.

We also mention an application to the theory of partial differential equations. Define the polynomial $Q(\eta_1,\eta_2)$ by setting

$$Q(\eta_1,\eta_2)=q(-2\pi i\eta_1,-2\pi i\eta_2)$$

and let E be a tempered distribution reciprocal to Q, so that $EQ=1$ (the existence of E is insured by our main result). Let F denote the Fourier transform operator

$$[Fu](x_1,x_2)=\int_{R^2}\exp[-2\pi i(x_1\eta_1+x_2\eta_2)]u(\eta_1,\eta_2)\,d\eta_1 d\eta_2,$$

for any $u\in(\zeta)$, and write $q(D)$ for the operation $q(\partial/\partial\eta_1,\partial/\partial\eta_2)$, $q(-D)$ for the operator $q(-\partial/\partial\eta_1,-\partial/\partial\eta_2)$. Then

$$[Fq(-D)u](x_1,x_2)=Q(x_1,x_2)\cdot\{[Fu](x_1,x_2)\}. \tag{1.1}$$

Define the tempered distribution S by the formula $S(u)=E(Fu)$, $u\in(\zeta)$. Then, by the way differentiation of a distribution is defined and by (1.1),

$$[q(D)S](u)=S[q(-D)u]=E(Fq(-D)u)=E(QFu)=[EQ](Fu).$$

But $EQ=1$ and since the distribution "1" at any function $w(x_1,x_2)$ of (ζ) takes the value $\int_{R^2}w\,dx_1dx_2$, we obtain, finally, by the Fourier inversion formula, that $[EQ](Fu)=\int_{R^2}F(u)\,dx_1dx_2=u(0)$. Therefore

$$q(D)S=\delta, \tag{1.2}$$

where δ is the Dirac distribution. Equation (1.2) says that S is an elementary solution for the operator $q(D)$. It follows, therefore, that in two dimensions every partial differential operator with constant coefficients has a tempered elementary solution.

This result improves (in the case of two dimensions) an earlier one due to Malgrange [3] and Ehrenpreis [1], who showed that any partial differential operator with constant coefficients in any number of variables possesses an elementary solution. The question was left open whether or not, as L. Schwartz originally conjectured, there exists a tempered elementary solution. Also, the elegant existence proofs of Malgrange and Ehrenpreis use the Hahn-Banach Theorem and give no indication how, for a given operator, its elementary solution may be constructed. Hörmander [2] has given an explicit formula for these untempered elementary solutions, but one which again is non-constructive (involving the analytic continuation of a Fourier transform). Therefore it appears that our method is the first, even in the

low dimension 2, which allows one to construct completely any kind of an elementary solution.

A different proof of these results was part of the author's doctoral dissertation at the University of Chicago [4]. The author would like to express his gratitude to Professor M. S. Stone for his long-continued help and interest.

Since this paper was written there has appeared a proof that the reciprocal of an analytic function of n real variables is a distribution (see M. S. Lojasiewicz, "Division d'une distribution par une function analytique de variables reelles," Comptes Rendus de l'academie des sciences de Paris, Tome 246, No. 5, February 1958). The general proof is unconstructive. It seems unlikely that it will ever be possible to construct the reciprocal of the most general analytic function (or even polynomial) in a number of dimensions greater than two.

2. Notation. Let $\eta = (\eta_1, \eta_2)$ be a real vector and let $q = q(\eta_1, \eta_2)$ be a polynomial in the variables η_1, η_2. We assume throughout this paper that the coefficients of q are real numbers and that q has degree greater than zero.[2] Let V be the real variety given by the equation $q(\eta_1, \eta_2) = 0$.

A point η^0 of V will be called unexceptional in case there exists a neighborhood U of η^0 and a pair of functions $v_1(\eta), v_2(\eta)$, analytic and with strictly positive Jacobian (with respect to η_1, η_2) in U, such that q is identically equal to some integral power of v_1 in U. A point of V not satisfying these requirements is called exceptional.

We say that q is irreducible if no polynomial of positive degree and with complex coefficients divides q; otherwise, we say q is reducible. A point η of V is called singular if both first partial derivatives of q vanish at η. Then, clearly, if q is irreducible, a point of V is exceptional if and only if it is a singular point.

If q is reducible, let $q = \prod_{i=1}^{\nu} [q_i]^{\alpha_i}$ be its decomposition into integral powers α_i of distinct irreducible polynomials q_i. Then it is easy to see that a point of V is exceptional if and only if it is either a singular point of some variety $q_i = 0$, $(i = 1, \cdots, \nu)$, or else belongs to the intersection of two or more of these varieties.

[2] The problem of finding the reciprocal of a complex polynomial Q can be reduced to the corresponding problem in the real case by means of the identity $Q^{-1} = Q^* \mid Q \mid^{-2}$, where Q^* is the conjugate, $\mid Q \mid$ the absolute value, of Q.

Assume now that we have chosen coordinates η_1, η_2 in such a way that their origin does not lie on V, and define polynomials $p, p_1, \cdots, p_\nu$ by setting $p(\eta_1, \eta_2, \lambda) \equiv q(\lambda\eta_1, \lambda\eta_2)$, $p_i(\eta_1, \eta_2, \lambda) \equiv q_i(\lambda\eta_1, \lambda\eta_2)$, $(i = 1, \cdots, \nu)$, and let

$$H(\eta_1, \eta_2) \equiv \prod_{\substack{i,j=1\\ i<j}}^{\nu} R_{ij} D_j, \tag{2.1}$$

where R_{ij} is the resultant of p_i and p_j, D_j the discriminant of p_j, where p_i and p_j are considered as polynomials in the variable λ. Since R_{ij} and D_j are homogeneous polynomials in the variables η_1 and η_2, the variety $H = 0$ is a cone with vertex at the origin. It is easy to see that every exceptional point of V will lie on the cone $H = 0$ as well as all points η^0 of V such that the line joining η^0 to the origin is tangent to V at η^0.

In order to save words later on, it is convenient to make the following convention. Let $g(\epsilon)$ be any complex-valued function defined in the interval $0 < \epsilon < \tau$. We shall write $g(\epsilon) = \infty(\epsilon)$ in case there exists a finite set M of negative fractions, complex numbers a and a_μ, $(\mu \in M)$, and a complex function $f(\epsilon)$ defined in the same interval as g such that $\lim_{\epsilon \to +0} f(\epsilon)$ exists and is finite and such that the equation

$$g(\epsilon) \equiv \sum_{\mu \in M} a_\mu \epsilon^\mu + a \log \epsilon + f(\epsilon) \tag{2.2}$$

hold for $0 < \epsilon < \tau$.

In case $g(\epsilon) = \infty(\epsilon)$, the complex number $\lim_{\epsilon \to +0} f(\epsilon)$ is uniquely determined and we shall denote it by $Pf. g(0)$.

3. A preliminary theorem.

THEOREM (3.1). *Let $q(\eta_1, \eta_2)$ be a real polynomial in the two real variables η_1, η_2 and let V be the variety $q = 0$. Let G be a region of R^2 the closure of which contains no exceptional points of V and let $G(\epsilon)$, $\epsilon > 0$, be that part of G where $|q| > \epsilon$. Then, for any u in (ζ),*

$$\int_{G(\epsilon)} u(\eta)[q(\eta)]^{-1} d\eta_1 d\eta_2 = \infty(\epsilon). \tag{3.2}$$

Proof. By means of a partition of unity, the integral on the left side of equation (3.2) is expressible as a sum of integrals of the form

$$\int_{U(\epsilon)} w(\eta)[q(\eta)]^{-1} d\eta_1 d\eta_2, \tag{3.3}$$

where $w(\eta)$ is a C^∞ function and where $U(\epsilon)$ is the intersection of $G(\epsilon)$

and a neighborhood U which is either disjoint from V or satisfies the conditions described in the definition of an unexceptional point. In the first case, the integral (3.3) has a finite limit. In the second, there exist coordinates v_1, v_2 in U such that $q \equiv (v_1)^a$ for some positive integer a. Setting

$$h(\epsilon) = \int_{W(\epsilon)} w(\eta(v)) J(v)\, dv_1,$$

where $W(\epsilon)$ is the part of the level surface $|q| = \epsilon$ lying in U and where $J(v)$ is the Jacobian of the coordinates $\eta = (\eta_1, \eta_2)$ with respect to the coordinates $v = (v_1, v_2)$, we get that

$$\int_{U(\epsilon)} w(\eta) [q(\eta)]^{-1} d\eta_1 d\eta_2 = \int_\epsilon^\infty h(\epsilon) \epsilon^{-a}\, d\epsilon.$$

Since $h(\epsilon)$ is C^∞, we may integrate by parts on the right side of the last equation and thereby obtain an expansion of the form (2.2). It follows that the integral on the left side of equation (3.2) is $\infty(\epsilon)$ since it is a sum of expressions each of which is $\infty(\epsilon)$. This proves Theorem (3.1).

4. The two main theorems. Let us again assume that $q(0,0) \neq 0$ and define the homogeneous polynomial $H(\eta_1, \eta_2)$ by equation (2.1). If we introduce polar coordinates ρ and θ in the usual way in the $\eta_1\eta_2$-plane, the cone $H = 0$ will be given by equations $\theta = \theta_1, \theta = \theta_2, \cdots, \theta = \theta_\Gamma$. If δ is a positive number, we let the region $G(\delta)$ consist of all points $(\rho\cos\theta, \rho\sin\theta)$ such that $|\theta - \theta_i| > \delta$, $(i = 1, 2, \cdots, \Gamma)$, and if ϵ is a second positive number we denote by $G(\delta, \epsilon)$ that part of $G(\delta)$ where $|q| > \epsilon$. For $u \in (\zeta)$, set

$$g_\delta(u;\epsilon) = \int_{G(\delta,\epsilon)} u(\eta) [q(\eta)]^{-1} d\eta. \tag{4.1}$$

By Theorem (3.1), $g_\delta(u;\epsilon) = \infty(\epsilon)$ for $\delta > 0$. Define, for $u \in (\zeta)$ and $\delta > 0$,

$$E(u;\delta) = Pf.\, g_\delta(u;0). \tag{4.2}$$

THEOREM (4.3). *Let $q(\eta_1, \eta_2)$ be a real polynomial such that $q(0,0) \neq 0$. For $u \in (\zeta)$ and $\delta > 0$, define $E(u;\delta)$ as above. Then $E(u;\delta) = \infty(\delta)$. Furthermore, if we set $E(u) = Pf.\, E(u;0)$, then E, considered as a functional on the function space (ζ), is a tempered distribution.*

THEOREM (4.4). *For any real polynomial q in two variables, there exists a tempered distribution E satisfying the equation $Eq = 1$.*

The proof of Theorem (4.3) will be found in the last part of this paper. Theorem (4.4) is a consequence of Theorem (4.3) as follows. We may assume

that the coordinates η_1, η_2 have been chosen in such a way that $q(0,0) \neq 0$. Then let E be the tempered distribution defined in Theorem (4.3). It must be shown that $Eq = 1$, or, what is the same thing, that $w \in (\zeta)$ implies that

$$E(qw) = \int_{R^2} w \, d\eta.$$

From equation (4.1), we get that

$$g_\delta(qw;\epsilon) = \int_{G(\delta,\epsilon)} w(\eta) \, d\eta,$$

and hence

$$E(qw;\delta) = Pf. \, g_\delta(u;0) = \int_{G(\delta)} w(\eta) \, d\eta,$$

so that

$$E(qw) = Pf. \, E(qw;0) = \int_{R^2} w(\eta) \, d\eta.$$

This proves Theorem (4.4).

5. Several lemmas. We assume $q(\eta_1, \eta_2)$ to be a polynomial such that $q(0,0) \neq 0$ and define $H(\eta)$ by equation (2.1).

LEMMA (5.1). *Let $\eta = (\eta_1, \eta_2)$ be a real vector such that $q(\eta) \neq 0$ and $H(\eta) \neq 0$. Then*

$$[q(\eta)]^{-1} = -\sum_{k=1}^{\sigma} a_k(\eta, \lambda_k),$$

where $\lambda_1, \cdots, \lambda_\sigma$ are the distinct roots of the equation $q(\lambda\eta_1, \lambda\eta_2) = 0$ and where $a_k(\eta, \lambda_k)$ is the residue of the function $[q(\lambda\eta_1, \lambda\eta_2)(\lambda - 1)]^{-1}$ of the complex variable λ at the point $\lambda = \lambda_k$.

Proof. By Cauchy's integral formula,

$$[q(\eta)]^{-1} = \frac{1}{2\pi i} \int_C [q(\lambda\eta_1, \lambda\eta_2)(\lambda - 1)]^{-1} \, d\lambda,$$

where C is a positively oriented circle with center at $\lambda = 1$ and radius small enough that C contains none of the points $\lambda_1, \cdots, \lambda_\sigma$ in its interior or on its circumference. $H(\eta) \neq 0$ implies that $q(\lambda\eta_1, \lambda\eta_2)$ is not constant in λ, and hence

$$\frac{1}{2\pi i} \int_{|\lambda|=R} [q(\lambda\eta_1, \lambda\eta_2)(\lambda - 1)]^{-1} \, d\lambda = 0$$

when R is greater than the maximum of the numbers $|\lambda_1|, \cdots, |\lambda_\sigma|$. The lemma then follows from the theorem of residues.

Remark (5.2). The number σ of distinct roots of the equation $q(\lambda\eta_1, \lambda\eta_2) = 0$ is constant in the region of R^2 where $H \neq 0$. See section 2.

LEMMA (5.3). *If* η *is as in Lemma* (5.1),

$$a_k(\eta, \lambda_k) = P_k(\eta, \lambda_k)\,[D^{m_k}p(\eta, \lambda_k)\,(\lambda_k - 1)]^{-m_k}$$

where P_k *is a polynomial in* λ_k *and* η, *where* $D = d/d\lambda$, *and where* m_k *is the multiplicity of* λ_k *considered as a zero of* $q(\lambda\eta_1, \lambda\eta_2)$. *Here* $k = 1, \cdots, \sigma$.

This lemma is proved by finding the coefficient of $(\lambda - \lambda_k)^{-1}$ in the Laurent expansion of the function $[q(\lambda\eta_1, \lambda\eta_2)(\lambda - 1)]^{-1}$ about $\lambda = \lambda_k$. We omit the short calculation.

It is convenient to let Ω denote the unit circle in the $\eta_1\eta_2$-plane and to denote by ξ_1, ξ_2 respectively the restrictions of η_1, η_2 to Ω. Let the single-valued algebraic function $\lambda_k(\xi)$ be a branch of the complete algebraic function $\lambda(\xi)$ defined on $\Omega(\xi)$ by the equations $q(\lambda\xi_1, \lambda\xi_2) = 0$ and $\xi_1{}^2 + \xi_2{}^2 = 1$.

LEMMA (5.4). *If* $\xi^0 \in \Omega$, *let* ξ_j, *where* $j = 1$ *or* 2, *be a coordinate function for* Ω *in a neighborhood of* ξ^0. *Then there exists a positive integer* h, *a determination* z *of* $(\xi_j - \xi^0{}_j)^{1/h}$ *and a positive number* τ *such that* $\lambda_k(\xi)$ *can be expanded in a convergent power series*

$$\lambda_k(\xi) = \sum_{i=0}^{\infty} b_i z^i \tag{5.5}$$

for $|z| < \tau$.

Proof. See Picard [5], Vol. II, Chap. 13.

6. The function $J_{\alpha\beta}(u; \xi, \lambda)$. Let A denote the complex λ-plane with the non-negative real axis removed. For $\lambda \in A$, $u \in (\zeta)$, and $\xi \in \Omega$, set

$$J_{\alpha\beta}(u; \xi, \lambda) = \int_0^\infty t^\alpha u(t\xi_1, t\xi_2)\,(\lambda - t)^{-\beta}\,dt$$

where α, β are any non-negative integers. When λ is a non-negative real number, the integral on the right need not converge, so that we must define $J_{\alpha\beta}$ somewhat differently in this case. For λ real, $\lambda > 0$, set

$$g(\epsilon) = \int_0^{\lambda-\epsilon} t^\alpha u(t\xi_1, t\xi_2)\,(\lambda - t)^{-\beta}\,dt + \int_0^{\lambda-\epsilon} t^\alpha u(t\xi_1, t\xi_2)\,(\lambda - t)^{-\beta}\,dt,$$

where ϵ is a positive number small enough that $\lambda - \epsilon > 0$. A repeated integration by parts of the two integrals on the right side of the above

equation shows that $g(\epsilon) = \infty(\epsilon)$, so that the number $Pf.\, g(0)$ is well defined. Set

$$J_{\alpha\beta}(u;\xi,\lambda) = Pf.\, g(0)$$

for all real positive λ. We leave $J_{\alpha\beta}$ undefined for $\lambda = 0$.

LEMMA (6.1). (i) *Restricted to positive real values of* λ, $J_{\alpha\beta}$ *is a* C^∞ *function of* λ, ξ_1 *and* ξ_2. (ii) $J_{\alpha\beta}$ *and all its partial derivatives with respect to* ξ_1 *and* ξ_2 *are regular analytic functions of* λ *for* $\lambda \in A$. (iii) *Let* a_0 *be a real number,* $a_0 > 0$, *and let* λ *approach the point* a_0 *in such a way that* $\operatorname{Im}\lambda$ *is non-zero and of constant sign. Then if* $P(d/d\lambda, \partial/\partial\xi)J_{\alpha\beta}$ *denotes an arbitrary partial derivative of* $J_{\alpha\beta}$ *with respect to* λ, ξ_1, *and* ξ_2, $P(d/d\lambda, \partial/\partial\xi)J_{\alpha\beta}$ *has a well-defined finite limit as* $\lambda \to a_0$.

Proof. (i) is verified by a straightforward calculation which we omit. (ii) follows at once from well-known theorems. We prove (iii). Since the expression $P(d/d\lambda, \partial/\partial\xi)J_{\alpha\beta}$ differs in no significant respect from $J_{\alpha\beta}$, it suffices to prove (iii) for the latter.

For $\lambda \in A$ and t in the interval $0 \leqq t < \infty$, we have that $0 < \arg(\lambda - t) < 2\pi$. For λ and t in these ranges, we define $\operatorname{Log}(\lambda - t) = \log|\lambda - t| + i\arg(\lambda - t)$. Then for $\lambda \in A$, we integrate by parts and obtain that

$$J_{\alpha\beta}(u;\xi,\lambda) = \sum_{k=-\beta+1}^{-1} c_k\lambda^k + c_0 \int_0^\infty \operatorname{Log}(\lambda - t) f(t\xi)\, dt + c_1 \operatorname{Log}\lambda,$$

where the c_k are certain complex numbers and $f(t\xi)$ is the β-th derivative of $t^\alpha u(t\xi_1, t\xi_2)$ with respect to t. Furthermore, we can write

$$\int_0^\infty \operatorname{Log}(\lambda - t) f(t\xi)\, dt = \int_0^\infty \log|\lambda - t|\, f(t\xi)\, dt + i\int_0^\infty \arg(\lambda - t) f(t\xi)\, dt. \tag{6.2}$$

Let $\lambda = a + bi$ and suppose $\lambda \to a_0$ in such a way that b is always positive. Clearly, the first integral on the right side of (6.2) tends to the limit $\int_0^\infty \log|a_0 - t|\, f(t\xi)\, dt$. If we define $h(t) = 0$ for $0 \leqq t < a_0$ and $h(t) = \pi$ for $a_0 \leqq t < \infty$, then the second integral on the right side of (6.2) tends to the limiting value $i\int_0^\infty h(t) f(t\xi)\, dt$ as $\lambda \to a_0$, since $\arg(\lambda - t)$ is bounded and converges uniformly to $h(t)$ as $|a - a_0| + b \to 0$ in every subset of the real line which excludes a neighborhood of the point a_0. This concludes the proof of (iii) and hence of the lemma.

Let $\xi^0 \in \Omega$ and let z be the function defined in Lemma (5.4). Then $z = \phi w$ where ϕ is an h-th root of unity and w is a real parameter lying in the interval $-\tau < w < \tau$.

LEMMA (6.3). (i) *There exists a positive number* τ *such that* $J_{\alpha\beta}(u;\xi,\lambda_k(\xi))$ *is infinitely differentiable with respect to* w *for* $0 < w < \tau$ *and for* $-\tau < w < 0$. *Furthermore, all derivatives of* $J_{\alpha\beta}(u;\xi,\lambda_k(\xi))$ *with respect to* w *are continuous in the half-closed intervals* $0 \leqq w < \tau$ *and* $-\tau < w \leqq 0$. (ii) $J_{\alpha\beta}$ *has the Taylor expansion*

$$J_{\alpha\beta}(u;\xi,\lambda_k(\xi)) = \sum_{j=0}^{n} d_j w^j + w^{n+1}K_n(w) \tag{6.4}$$

for $0 \leqq w < \tau$, *where* n *is any positive integer, the* d_j *are complex numbers,* $K_n(w)$ *is infinitely differentiable for* $0 < w < \tau$ *and all its derivatives are continuous in the half-closed interval* $0 \leqq w < \tau$. (iii) *An expansion similar to* (6.4) *exists in the interval* $0 \geqq w > -\tau$.

Proof. (ii) and (iii) follow immediately from (i), so we prove only the latter. For the sake of brevity, we restrict ourselves to showing the existence of an interval $0 < w < \tau$ where (i) is true; a repetition of the argument will prove (i) for small negative values of w. We choose τ small enough that $\lambda_k(\xi(w))$ is either everywhere real or everywhere non-real in the interval $0 < w < \tau$. If λ_k is real for $0 \leqq w < \tau$, then (i) follows from Lemmas (5.4) and (6.1) since a composition of differentiable functions is differentiable. The same argument applies in the other two possible cases as well, except that if λ_k is real for $w = 0$ but non-real for $w \neq 0$, the derivatives of $J_{\alpha\beta}$ may have a jump discontinuity at $w = 0$. But in any case, they have well-defined finite limits as $w \to 0$. This proves Lemma (6.3).

Let $\Omega(\delta)$, for small positive δ, denote the intersection of the region $G(\delta)$ with the unit circle Ω and for small positive ϵ let $S(\epsilon,\theta)$ denote that part of the interval $0 \leqq t < \infty$ where $|q(t\cos\theta, t\sin\theta)| > \epsilon$. Then for $\epsilon > 0$ and θ such that $(\cos\theta,\sin\theta) \in \Omega(\delta)$, set

$$w(\epsilon,\theta) = \int_{S(\epsilon,\theta)} t^{\alpha} u(t\cos\theta, t\sin\theta)\,(\lambda_k(\theta) - t)^{-\beta}\,dt, \tag{6.5}$$

where $\lambda(\theta)$ is a solution of the equation $q(\lambda_k(\theta)\cos\theta, \lambda_k(\theta)\sin\theta) = 0$ and α, β are arbitrary non-negative integers.

LEMMA (6.6). *Let* $C(\delta)$ *be the closure of some component of* $\Omega(\delta)$. *Then there exists a positive number* ϵ_0, *a finite set* M *of negative fractions, functions* $c_\mu(\theta)$, *where* μ *runs over* M, *and functions* $c(\theta)$, $d(\theta,\epsilon)$ *such that:* (i)

$c_\mu(\theta)$, $c(\theta)$ are defined and continuous for all θ such that $(\cos\theta, \sin\theta) \in C(\delta)$; (ii) $d(\theta,\epsilon)$ is defined and continuous in both θ and ϵ for θ such that $(\cos\theta, \sin\theta) \in C(\delta)$ and $0 \leqq \epsilon < \epsilon_0$; (iii) $w(\epsilon,\theta) = \sum_{\mu\in M} c_\mu(\theta)\epsilon^\mu + c(\theta)\log\epsilon + d(\theta,\epsilon)$ for all such values of ϵ and θ.

Proof. Since by assumption $q(0,0) \neq 0$, we can choose a positive number γ_0 such that $q(0,0) \neq \tau$ whenever τ is a real number satisfying the inequality $|\tau| < \gamma_0$. For real τ, let

$$q(\eta_1,\eta_2) - \tau = \prod_{i=1}^{\nu} [q_i(\eta_1,\eta_2;\tau)]^{\alpha_i}$$

be a decomposition of $q(\eta_1,\eta_2) - \tau$, considered as a polynomial in η_1 and η_2, into integral powers α_i of irreducible polynomials $q_i(\eta_1,\eta_2;\tau)$ and let $D_j(\eta_1,\eta_2;\tau)$ be the discriminant of the polynomial $q_j(\lambda\eta_1,\lambda\eta_2;\tau)$, $R_{ij}(\eta_1,\eta_2;\tau)$ the resultant of the polynomials $q_i(\lambda\eta_1,\lambda\eta_2;\tau)$ and $q_j(\lambda\eta_1,\lambda\eta_2;\tau)$ where these latter are considered as polynomials in λ alone. Then set

$$H(\eta_1,\eta_2;\tau) = \prod_{\substack{i,j=1\\ i<j}}^{\nu} R_{ij}(\eta_1,\eta_2;\tau) D_j(\eta_1,\eta_2;\tau).$$

$H(\eta_1,\eta_2;\tau)$ is homogeneous in η_1, η_2, so that $H = 0$ is a cone. By the definition of H, a line through the origin belongs to this cone if it is tangent to or passes through an exceptional point of the curve $q = \tau$.

Let $\Gamma(\delta)$ denote the angular sector of R^2 consisting of all points which lie on a line passing through both the origin and a point of $C(\delta)$. We have that $H(\eta_1,\eta_2;0)$ vanishes in $\Gamma(\delta)$ at just the point $\eta_1 = \eta_2 = 0$. Since $H(\eta_1,\eta_2;\tau)$ is a continuous function of τ and homogeneous in η_1 and η_2 we can choose a positive number γ_1 less than γ_0 and such that for $|\tau| < \gamma_1$ the polynomial $H(\eta_1,\eta_2;\tau)$ does not vanish in $\Gamma(\delta)$ except at the origin.

Now let V_τ denote the curve $q = \tau$ and consider that part of it lying in $\Gamma(\delta)$. By our construction, if $|\tau| < \gamma_1$, $V_\tau \cap \Gamma(\delta)$ will consist of a number of disjoint components $V_\tau^1, \cdots, V_\tau^s$, each of which is non-singular and nowhere tangent to a line passing through the origin. If ρ denotes the radial distance from the origin, V_τ^i will be given by the equation $\rho = \rho^i(\tau,\theta)$ where ρ^i is an analytic function of τ and θ for $|\tau| < \gamma_1$, θ such that $(\cos\theta, \sin\theta) \in C(\delta)$. Furthermore, since the components $V_\tau^1, \cdots, V_\tau^s$ are disjoint, we may assume that $0 < \rho^1(\tau,\theta) < \cdots < \rho^s(\tau,\theta)$. From the definition of $\lambda_k(\theta)$, we see that there are two possible cases: (i) $\lambda_k(\theta) \neq \rho^i(0,\theta)$ for $i = 1, \cdots, s$ and all θ such that $(\cos\theta, \sin\theta) \in C(\delta)$; (ii) there exists a unique integer j, $1 \leqq j \leqq s$, such that $\lambda_k(\theta) \equiv \rho^j(0,\theta)$ while $\lambda_k(\theta) \neq \rho^i(0,\theta)$

for $i=1,2,\cdots,j-1,j+1,\cdots,s$ and all θ such that $(\cos\theta,\sin\theta)\in C(\delta)$.

In the first case, there is nothing to prove since $w(\epsilon,\theta)$ will then be continuous at $\epsilon=0$. So assume (ii) holds. Then $V_0{}^j$ will be flanked by two curve segments, one from the family $V_\epsilon{}^i$ and one from the family $V_{-\epsilon}{}^i$. It is convenient to choose our notation in such a way that $V_{-\epsilon}{}^i$ is given by the equation $\rho=\rho(-\epsilon,\theta)$, $V_0{}^j$ by the equation $\rho=\rho(0,\theta)$, and $V_\epsilon{}^i$ by the equation $p=p(\epsilon,\theta)$. Without loss of generality, we can assume that $\rho(-\epsilon,\theta)<\rho(0,\theta)<\rho(\epsilon,\theta)$ for ϵ positive, $\epsilon<\gamma_2<\gamma_1$, and for θ such that $(\cos\theta,\sin\theta)\in C(\delta)$. This being so, we have that

$$(6.7)\qquad w(\epsilon,\theta)=\int_0^{\rho(-\epsilon,\theta)} t^\alpha u(t\cos\theta,t\sin\theta)(\lambda_k(\theta)-t)^{-\beta}\,dt \\ +\int_{\rho(\epsilon,\theta)}^{\infty} t^\alpha u(t\cos\theta,t\sin\theta)(\lambda_k(\theta)-t)^{-\beta}\,dt+W(\epsilon,\theta),$$

where $W(\epsilon,\theta)$ is continuous for $0\leqq\epsilon<\gamma_2$ and θ such that $(\cos\theta,\sin\theta)\in C(\delta)$ and where $W(0,\theta)\equiv 0$. It therefore suffices to prove that the integrals appearing on the right side of equation (6.7) have an expansion of the form required by (iii) of the lemma. We consider only the first integral and denote it by $w_1(\epsilon,\theta)$; the second integral can be treated in an analogous manner. Setting $f(t,\theta)\equiv t^\alpha u(t\cos\theta,t\sin\theta)$ and integrating by parts β times, we obtain

$$(6.8)\qquad w_1(\epsilon,\theta)=\sum_{i=1}^{\beta-1} b_i f^{(i-1)}(\rho(-\epsilon,\theta),\theta)(\lambda_k(\theta)-\rho(-\epsilon,\theta))^{i-\beta} \\ +b_0 f^{(\beta-1)}(\rho(-\epsilon,\theta)\log|\lambda_k(\theta)-\rho(-\epsilon,\theta)| \\ +b\int_0^{\rho(-\epsilon,\theta)} f^{(\beta)}(\rho(-\epsilon,\theta)\log|\lambda_k(\theta)-\rho(-\epsilon,\theta)|\,dt \\ +\cdots,$$

where $+\cdots$ indicates that we have omitted those boundary terms (independent of ϵ) which arise from the limit of integration $t=0$, where b_i, b_0, b are constants and where $f^{(i)}$ denotes the i-th partial derivative of f with respect to t.

Now the function $\rho(\epsilon,\theta)$ satisfies the equation

$$q_i(\rho(\epsilon,\theta)\cos\theta,\rho(\epsilon,\theta)\sin\theta)=\epsilon$$

for some irreducible polynomial q_i and hence

$$\partial\rho/\partial\epsilon=[(\partial q_i/\partial\eta_1)\cos\theta+(\partial q_i/\partial\eta_2)\sin\theta]^{-1}.$$

Therefore $|\partial\rho/\partial\epsilon|\geqq|\operatorname{grad} q_i|^{-1}>0$. It follows that we can write

$$[\lambda_k(\theta)-\rho(-\epsilon,\theta)]^{-1}\equiv\epsilon^{-1}\pi(\epsilon,\theta)$$

for $\epsilon < \epsilon_0 < \gamma_2$ and for all θ such that $(\cos\theta, \sin\theta) \in C(\delta)$ and where $\pi(\epsilon, \theta)$ is analytic for these values of ϵ and θ.

For such values of ϵ and θ, the integral on the right side of equation (6.8) is obviously continuous. Consider the remaining terms on the right side of this equation. Each has an expansion of the kind required by (iii) of the lemma, since $f^{(i-1)}(\rho(-\epsilon,\theta),\theta)$ is infinitely differentiable in ϵ and can be expanded in a Taylor's expansion in ϵ about $\epsilon = 0$, while by what we have said above, the quantity $[\lambda_k(\theta) - \rho(-\epsilon,\theta)]^{i-\beta}$ can be expanded in a series of negative and positive powers of ϵ and the coefficients of both expansions will be continuous functions of θ as desired. Therefore $w_1(\epsilon,\theta)$ has an expansion of the form (iii). This proves Lemma (6.6).

We recall that for $u \in (\zeta)$ and for $\delta > 0$, the number $E(u;\delta)$ is defined by equation (4.2).

LEMMA (6.9). *$E(u,\delta)$ is equal to a linear combination of terms of the form*

$$(6.10) \qquad \int_{\Omega(\delta)} R(\theta) J_{\alpha\beta}(u; \xi(\theta), \lambda_k(\theta))\, d\theta,$$

where α, β are non-negative integers and for some other non-negative integers i, j_1, j_2,

$$R(\theta) = [\lambda_k(\theta)]^i [\xi_1(\theta)]^{j_1} [\xi_2(\theta)]^{j_2} [D^{m_k} p(\xi(\theta), \lambda_k(\theta))]^{-m_k}$$

where $D = (d/d\lambda)$ and where m_k is the multiplicity of $\lambda_k(\theta)$ considered as a root of the equation $p(\xi(\theta), \lambda_k(\theta)) = 0$.

Proof. By definition (equation (4.1)), $g_\delta(u;\epsilon) = \int_{G(\delta,\epsilon)} u(\eta)[q(\eta)]^{-1}\, d\eta$. Then by Lemmas (5.1) and (5.3), $g_\delta(u;\epsilon)$ is a linear combination of expressions of the form:

$$(6.11) \qquad \int_{G(\delta,\epsilon)} u(\eta)\eta_1^{j_1}\eta_2^{j_2}[\lambda_k(\eta)]^i [D^{m_k} p(\eta, \lambda_k(\eta))(\lambda_k(\eta) - 1)]^{-m_k}\, d\eta.$$

Introducing polar coordinates $\eta_1 = t\cos\theta$, $\eta_2 = t\sin\theta$, and using the formula $\lambda_k(\eta_1,\eta_2) = t^{-1}\lambda_k(\cos\theta, \sin\theta) = t^{-1}\lambda_k(\theta)$, we find that

$$D^{m_k} p(\eta, \lambda_k(\eta)) = t^{m_k} D^{m_k} p(\cos\theta, \sin\theta, \lambda_k(\theta)).$$

Hence (6.11) becomes

$$(6.12) \qquad \int_{\Omega(\delta)} R(\theta)\, d\theta \int_{S(\epsilon,\theta)} t^{\alpha} u(t\cos\theta, t\sin\theta)(\lambda_k(\theta) - t)^{-m_k}\, dt,$$

where $\alpha = j_1 + j_2 - i + m_k(1 - m_k) + 1$ and where $S(\epsilon,\theta)$ is that part of the interval $0 \leqq t < \infty$ where $|q(t\cos\theta, t\sin\theta)| > \epsilon$.

Keeping δ fixed always, let $h(\epsilon)$ denote the expression (6.12). To prove Lemma (6.9), we must show that $h(\epsilon) = \infty(\epsilon)$ and further that

$$Pf.\,h(0)=\int_{\Omega(\delta)} R(\theta)J_{\alpha\beta}(u;\xi(\theta),\lambda_k(\theta))\,d\theta,$$

where we have put $\beta=m_k$. Define $w(\epsilon,\theta)$ as in equation (6.5). Then, by Lemma (6.6), we can write $w(\epsilon,\theta)=\sum_{\mu\in M} c_\mu(\theta)\epsilon^\mu+c(\theta)\log\epsilon+d(\theta,\epsilon)$. Then

$$h(\epsilon)=\sum_{\mu\in M}\epsilon^\mu\int_{\Omega(\delta)} R(\theta)c_\mu(\theta)\,d\theta+\log\epsilon\int_{\Omega(\delta)} R(\theta)c(\theta)\,d\theta$$
$$+\int_{\Omega(\delta)} R(\theta)\,d(\theta,\epsilon)\,d\theta.$$

From this equation, it follows that

$$Pf.\,h(0)=Pf.\{\int_{\Omega(\delta)} R(\theta)\,d(\theta,\epsilon)\,d\theta\}_{\epsilon=0},$$

provided the quantity in brackets on the right has a finite limit as $\epsilon\to 0$. However, this is the case since, by Lemma (6.6), $d(\theta,\epsilon)$ is continuous, and therefore

$$\lim_{\epsilon\to 0}\int_{\Omega(\delta)} R(\theta)\,d(\theta,\epsilon)\,d\theta=\int_{\Omega(\delta)} R(\theta)\,[\lim_{\epsilon\to 0} d(\theta,\epsilon)\,]\,d\theta.$$

This proves Lemma (6.9).

7. Proof of Theorem (4.3). This theorem states that $E(u;\delta)=\infty(\delta)$. By Lemma (6.9), it suffices to show that an expression of the form (6.10) is $\infty(\delta)$ and this in turn amounts to showing that

$$\int_{\theta^0+\delta}^{\theta^0+\tau} R(\theta)J_{\alpha\beta}(u;\xi(\theta),\lambda_k(\theta))\,d\theta=\infty(\delta), \tag{7.1}$$

where θ^0 is a solution of the equation $H(\cos\theta^0,\sin\theta^0)=0$ and where τ is a positive number such that $\tau>\delta$ and so small that the interval $\theta^0<\theta<\theta^0+\tau$ contains no solution of this equation. Let $\xi_1{}^0=\cos\theta^0$, $\xi_2{}^0=\sin\theta^0$ and define the parameter w on Ω as in Lemma (6.3). By equation (5.5), equation (6.4), and the definition of $R(\theta)$, we can write

$$R(\theta)J_{\alpha\beta}(u;\xi(\theta),\lambda_k(\theta))\,d\theta=\{\sum_{\mu\in M}\gamma_\mu w^\mu+\gamma\log|w|+c(w)\}dw, \tag{7.2}$$

where γ_μ, γ are numbers independent of w, M is a finite set of negative fractions, and $c(w)$ is continuous for those values of w corresponding to the interval $\theta^0\leqq\theta<\theta^0+\delta$. Substituting the expansion (7.2) inside the interval on the left side of equation (7.1) and integrating term by term, we prove equation (7.1) and hence that $E(u;\delta)=\infty(\delta)$.

The proof of Theorem (4.3) will be complete if we show that, considered as a functional on the space (ζ), E is a tempered distribution. It is obvious

that E is linear, so we need only establish its continuity. We consider a sequence $\{u_n\}$ where u_n is a C^∞ function of η_1, η_2 which tends to zero in the sense that for an arbitrary polynomial $P(\eta_1, \eta_2)$ and an arbitrary but fixed partial derivative D, the sequence $\{PDu_n\}$ tends to zero uniformly in R^2. To show the continuity of E, it suffices to show that $E(u_n) \to 0$ as $n \to \infty$.

Under these assumptions concerning the sequence $\{u_n\}$, we shall have that $J_{\alpha\beta}(u_n; \xi, \lambda) \to 0$ for all fixed ξ and λ and the convergence is uniform for $\xi \in \Omega$, $\lambda \neq 0$. This follows from the definition of $J_{\alpha\beta}$. Moreover, the statement remains true if we replace $J_{\alpha\beta}$ by $D_1 J_{\alpha\beta}$, where D_1 represents any partial differentiation with respect to ξ and λ.

By Lemma (6.9), we shall be finished if we verify that the expression

$$\int_{\Omega(\delta)} R(\theta) J_{\alpha\beta}(u_n; \xi(\theta), \lambda_k(\theta))\, d\theta \tag{7.3}$$

tends to zero as $n \to \infty$. But by formula (7.2), we have that

$$R(\theta) J_{\alpha\beta}(u_n; \xi(\theta), \lambda_k(\theta))\, d\theta = \{ \sum_{\mu \in M} \gamma_\mu w^\mu + \gamma \log |w| + c(w) \} dw.$$

Since the γ_μ, γ all contain a derivative of $J_{\alpha\beta}$ as a factor, they tend to zero as $n \to \infty$. The function $c(w)$ contains as a factor the remainder term of a Taylor's expansion of $J_{\alpha\beta}$ about $w = 0$. Since all derivatives of $J_{\alpha\beta}$ converge uniformly to zero as $n \to \infty$, it follows that the integral of $c(w)$ will tend to zero as $n \to \infty$. Hence (7.3) tends to zero as $n \to \infty$. This proves that E is continuous, and therefore Theorem (4.3) is established.

UNIVERSITY OF CHICAGO,
WESLEYAN UNIVERSITY, MIDDLETOWN, CONN.

REFERENCES.

[1] L. Ehrenpreis, "Solution of some problems of division," *American Journal of Mathematics*, vol. 76 (1954), pp. 883-903.

[2] L. Hörmander, Mimeographed Report, University of Chicago, 1956.

[3] B. Malgrange, "Equations aux derivees partielles a coefficients constants," *Comptes Rendus Hebdomadaires des Séances de l'Academie des Sciences*, vol. 237 (1953), pp. 1620-1622.

[4] J. McKibben, *Divergent integrals and elementary solutions*, doctoral dissertation, University of Chicago, June 1957.

[5] E. Picard, *Traite d'Analyse*, Gauthier-Villars and Cie., Paris, 1925.

[6] L. Schwartz, *Theorie des Distributions*, Hermann and Cie, Paris, vol. 1 (1950), vol. 2 (1951).

LINEAR DIFFERENTIAL EQUATIONS WITH ALMOST PERIODIC COEFFICIENTS.*

By JAMES C. LILLO.[1]

Introduction. We shall be interested in linear systems of the form $x' = A(t)x + B(t)$, where $A(t)$ is an $n \times n$ matrix, $B(t)$ is an n vector, and their entries are almost periodic functions (either real or complex valued). Historically, the approach to this type of problem has been to assume that the solutions of the system $x' = A(t)x$ have certain properties and then obtain the existence of an almost periodic solution of $x' = A(t)x + B(t)$. The limitations of such a procedure are apparent. While the results obtained in this paper are restricted to rather special types of almost periodic matrices, they do possess the advantage that the restrictions are placed directly upon the coefficients. For the case $B \equiv 0$, we shall concern ourselves with a modified form of the representation problem considered by Cameron [4]. Our results divide into two main types, the first type being when $A(t)$ is a superdiagonal matrix. An example (example A) is obtained which illustrates the difficulties involved and suggests the restrictions imposed in Theorem 1. The second type of matrix $A(t)$ considered is that in which the frequencies of the $a_{ij}(t)$ are all positive and bounded away from zero. The results in this case are an extension of earlier results due to Wintner and Putnam [12]. For the case $B \not\equiv 0$, we consider the existence of almost periodic solutions. The main result is found in Theorem 3. We shall employ the notation used by Besicovitich [1], writing a. p. for almost periodic and denoting the unique association of an a. p. function with its Fourier series by $\sim$.

Part I. We consider here systems of the form 1) $x' = A(t)x$, where $A(t)$ is an $n \times n$ matrix of a. p. functions. A classical question for systems of this type is when may the fundamental solution be written in the form $\phi(t) = P(t)\exp(At)$, where $P(t)$ is an a. p. matrix and A is a constant

* Received April 24, 1958.

[1] The above research was done while the author was a member of the O. N. R. project in differential equations at Princeton University. It comprises a part of the author's Ph. D. thesis at Princeton University. In this regard, the author wishes to thank his advisor, Professor S. Lefschetz, for his continual encouragement and advice.

matrix. We consider here a slightly more general representation problem. We ask when the components of every solution of 1) may be written in the form $\exp(\lambda_j)\sum_{l=0}^{k} t^l/l!\,P_l(t)$, where $P_l(t)$ is a. p. and k is equal to or less than the multiplicity of λ_j. We consider first the case in which the matrix $A(t)$ is superdiagonal. The results of Perron [10] and Diliberto [5] assure us that any equation $x' = D(t)x$, where $D(t)$ is bounded and continuous, is kinematically [8] similar to an equation of the form $x' = A(t)x$, where $A(t)$ is superdiagonal. Unfortunately, it is not known under what conditions the resulting $A(t)$ will be almost periodic when the $B(t)$ is so restricted. Thus for the present at least, the restriction to the superdiagonal is a serious limitation. The results obtained, however, are quite complete, and example A in particular has rather interesting implications. In preparation for the study of superdiagonal systems, we have the following three lemmas.

LEMMA 1. *If* $p(t) \sim \sum_{j=1}^{\infty} a_j \exp(i\Lambda_j t)$ *is an* a. p. *function and* $\operatorname{Re}\lambda > 0$, *then*

$$q(t) = \int_t^{\infty} p(s)\exp[\lambda(t-s)]\,ds \text{ is a. p. and } q(t) \sim \sum_{j=1}^{\infty} a_j \exp(i\Lambda_j t)/(\lambda + i\Lambda_j).$$

Proof. The a. p. nature of $q(t)$ was established by Murray [9]. The nature of the Fourier development of $q(t)$ may be obtained by a simple generalization of the technique used by Bohr [3] to show the analogous fact for the integral of a. p. functions.

LEMMA 1′. *If* $p(t) \sim \sum_{h=1}^{\infty} a_h \exp(i\Lambda_h t)$ *is an* a. p. *function and* $\operatorname{Re}\lambda > 0$, *then* $\int_t^{\infty} p(s)[(t-s)^m t^l \exp[\lambda(t-s)]]/(m!\,l!)\,ds = \sum_{j=0}^{l} (t^j/j!)\,q^j(t)$, *where each* $q^j(t)$ *is* a. p., $q^j(t) \sim \sum_{h=1}^{\infty} [a_h/(\lambda + i\Lambda_h)^{m+1+j}]\exp(i\Lambda_h t)$. *Furthermore, if* $M = \text{l. u. b.}\,|p(t)|$, *the* l. u. b. $|q^j(t)| \leqq 2M/\lambda^{m+1}$.

Proof. The result is established in essentially the same way as Lemma 1.

LEMMA 2. *Given any* a. p. *function* $b(t) \sim \sum_{j=1}^{\infty} b_j \exp(i\Lambda_j t) + b_0$, *where* $|\Lambda_j - \Lambda_i| > \delta > 0$ $(j \neq i)$, $|\Lambda_i| > \delta > 0$, *there exists an* a. p. *function* $h(t) \sim \sum_{l=1}^{\infty} h_l \exp(+\gamma_l t)$, *where* $|\gamma_l - \gamma_{l+1}| > \delta/2$ *and* $|\gamma_l| > \delta/2 > 0, i, l = 1, 2, \cdots$, *such that* $\int_0^t b(s)h(s)\,ds = f(t)$ *is not an* a. p. *function.*

Proof. Define $\gamma_j = [-\Lambda_j + b_j h_j/(j+k)^2]$ where h_j are chosen so that $b_j h_j \neq b_k h_k$ $(j \neq k)$, $\sum_{l=0}^{\infty} | h_l |^2$ is bounded, and k is a positive integer such that l. u. b. $| b_j h_j |/k^2 < \delta/4$. Then $h(t)$ is an a. p. function and its indefinite integral is also an a. p. function. We now establish the fact that the integral of $b(t)h(t)$ is not a. p. Now

$$b(t)h(t) \sim [\sum_{j=1}^{\infty} b_j \exp(i\Lambda_j t) + b_0][\sum_{l=1}^{\infty} h_l \exp(-i\gamma_l t)],$$

and so, if the indefinite integral of $b(t)h(t)$ were an a. p. function, by known results, its Fourier development would have to be similar to that obtained by formally integrating the above formal product. However, if one formally does this, he obtains a Fourier series $\sum_{l,j=1}^{\infty} c_{lj} \exp[(i\Lambda_j \gamma_l)t]$ for which the partial sums $\sum_{l,j=1}^{\infty} (| c_{lj} |)^2$ are unbounded. Thus we may conclude that the integral of the product $b(t)h(t)$ is not an a. p. function.

We here note that it is possible to restrict oneself to real a. p. functions and still obtain the results of Lemma 2. The necessary modifications are suggested by the trigonometric identity: $(\cos\Lambda_n + \sin\Lambda_n)(\cos\gamma_n - \sin\gamma_n) = \cos(\Lambda_n + \gamma_n) + \sin(\Lambda_n - \gamma_n)$. In this connection, it is noted that the example which appears in the following paragraph may be similarly modified.

Consider now the linear system of the form $x' = A(t)x$, where $A(t)$ is a. p. and superdiagonal. We begin by using the results obtained in Lemma 2, to construct an example which illustrates the difficulties involved even for very special systems. Upon considering this example, the hypotheses of Theorem 1 and its corollary are immediately suggested.

Example A. We consider the linear system in two variables of the form:

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} a_1(t) & a_2(t) \\ 0 & b_1(t) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

where the functions $a_1(t)$ and $b_1(t)$ are periodic 2π and mean M. Therefore $\int_0^t a_1(s)\,ds = Mt + h(t)$ and $\int_0^t b_1(s)\,ds = Mt + c(t)$, where $c(t)$ and $h(t)$ are periodic with zero mean. We have that $(\exp(Mt + h(t)), 0)$ and

$$(\exp(Mt + h(t)) \cdot [1 + \int_0^t \exp(-h(s) + c(s)) \cdot a(s)\,ds], \exp(Mt + c(t)))$$

form a basis for the solution space. Since $\exp[-h(t) + c(t)]$ is periodic, it clearly satisfies the conditions of Lemma 2 for $b(t)$ so that if we define $a_2(t)$ as the corresponding $h(t)$ of Lemma 2, then the given system will not admit a representation of the desired form.

Since, upon repeated integration of the functions $a_1(t) - M$, $b_1(t) - M$, and $a_2(t)$, we always obtain an a. p. function, it is clear that the imposing of integrability conditions on the $a_{ij}(t)$ will not suffice to give a representation result. A spacing condition on the frequencies is likewise seen to be adequate. The results of Lemma 1 suggest, of course, that a restriction be put on the integrability and mean values of the diagonal terms. This is done in the following theorem.

THEOREM 1. *If the system* $x' = A(t)x = (a_{ij}(t))x$ *satisfies* 1) $a_{ij}(t) \equiv 0$ *for* $i < j$, 2) *the* $a_{ij}(t)$ *are* a. p., 3) $\int_0^t a_{ii}(s)\,ds = m_i t + p_i(t)$, *where* $p_i(t)$ *is* a. p. *and* $m_i \neq m_j$ *for* $i \neq j$, *then there exists a fundamental set of solutions* $x_1(t), \cdots, x_n(t)$, *where* $x_h{}^j(t) = \exp(m_h t) \sum_{i=1}^{h} P_{hj}{}^i(t)$, $j \leqq h$; $x_h{}^j(t) = 0$, $j > h$. *Here the* $P_{hj}{}^i(t)$ *are* a. p. *with their module contained in that of* $A(t)$.

Proof. This result is an immediate consequence of repeated applications of Lemma 1.

COROLLARY. *If, in addition to the hypothesis of Theorem* 1, *we insist that the* m_i *be lineary ordered and that no solution* $x(t)$ *having an exponential multiplier* $\exp(\lambda t)$ *be such that* $\exp(-\lambda t)x(t)$ *is bounded and positive twistable with respect to the module of* A, *then any fundamental solution* $\Phi(t)$ *of* $x' = A(t)x$ *has a representation of the form* $\Phi(t) = P(t)\exp(At)$, *where* A *is a constant matrix and* $P(t)$ *is an* a. p. *matrix whose module is contained in the module of* $A(t)$.

Proof. The proof is a straightforward application of Theorem XIII of Cameron's paper [4].

We next consider linear systems of the form 1) where the $a_{ij}(t)$ are a. p. functions whose frequencies are all positive (or all negative) and bounded away from zero. This type of system was first considered by Putnam and Wintner [12] in the special case of a second order equation. Their results were extended by S. Sandor [11] to the case of an n-th order equation. In Theorem 2, we extend these results to general n-dimensional linear systems.

Thus we consider the system $x' = A(t)x$, where $A(t) = (a_{ij}(t))$ and the $a_{ij}(t)$ are a. p. functions having frequencies which are all of the same sign, say positive, and bounded away from zero. Let Λ denote the g. l. b. of the absolute values of the frequencies of the $a_{ij}(t)$. We may assume, without loss of generality, that $\Lambda > 2$ (i. e. a change of parameter will make it such). Let A_0 denote the matrix formed by the constant terms of the $a_{ij}(t)$. We insist that the imaginary parts of the roots λ_j of A_0 are less than Λ so, as above, we may assume $\gamma = \min(\Lambda\text{-}\operatorname{Im}\lambda) > 2$.

THEOREM 2. *Corresponding to each solution of* $x' = A_0x$ *of the form* $\exp(\lambda_i t)[0,\cdots,0,t^m/m!,0,\cdots,0]$, *the system* $x' = A(t)x$, *as defined above, has a solution each of whose components are of the form* $\exp(\lambda_i t)\sum_{l=0}^{m} t^l/l!\,p_l(t)$, *where the* $p_l(t)$ *are* a.p. *functions whose module is contained in the module of* $(A(t), \operatorname{Im}\lambda_j)$.

Proof. In this proof, we assume the frequencies are all positive since, by a change of parameter, this is always possible. Let $a(t)$ denote a general $a_{ij}(t)$. We shall be interested only in general properties of the $a_{ij}(t) \sim \sum_{l=1}^{m} c_l \exp(i\Lambda_l t)$. Thus for $\int_t^\infty \exp[\delta(t-s)]\cdot a_{ij}(s)\,ds \sim \sum_{l=1}^{\infty} c_l \exp(i\Lambda_l t)/(\delta + i\Lambda_l)$, we simply write $a(t)/\Lambda$. Similarly, for $\int_t^\infty \exp(t-s))\cdot a(s)\cdot a(s)/\Lambda\,ds$, we simply write $a^2(t)/(2!\Lambda^2)$, where the frequencies of $a^2(t)$ all exceed 2Λ. In the case of simple roots, we have, corresponding to the solution $x = \exp(\lambda_h t)[0,\cdots,0,1,0,\cdots,0]$ of the system $x' = A_0x$, the solution $x(t) = x^0(t) + \sum_{l=1}^{\infty} x^l(t)$ of the system $x' = A(t)x$. Here $x^0(t) = \exp(\lambda_h t)[0,\cdots,1,0,\cdots,0]$, and the components of $x^l(t)$ are defined in terms of the components of $x^{l-1}(t)$ as follows for $j \neq h$: $x^l{}_j(t) = \exp(\lambda_j t)\int \exp(-\lambda_j s)\sum_{m=1}^{n} a_{mj}(t)x^{l-1}{}_m(s)\,ds$. If the real part of $(-\lambda_j + \lambda_h)$ is < 0 $[> 0]$, then the limits of integration in the above definition are taken as $\int_\infty^t$ $[\int_{-\infty}^t]$. For $x^l{}_h(t)$, we have

$$x^l{}_h(t) = \exp(\lambda_h t)[c^l + \int_0^t \exp(-\lambda_h s)\sum_{m=1}^{n} a_{im}(s)x^{l-1}{}_m(s)\,ds],$$

where c^l is the value of the integral at its lower limit of integration. Thus $x^1{}_j(t) = [a(t)/(\lambda_h - \lambda_j + i\Lambda)]\exp(\lambda_h t)$ and $x^1{}_h(t) = [a(t)/(i\Lambda)]\exp(\lambda_h t)$. In what follows, for convenience, we drop the $\lambda_h - \lambda_j + i\Lambda$ and simply write γ. Now assume $x^q{}_j(t) = n^{q-1}a^q(t)\exp(\lambda_h t)/(q!\gamma^q)$, where $a^q(t)$ is an a.p. function with no constant term and whose least frequency is greater than $q\gamma$. Then:

$$x^{q+1}{}_j(t) = \exp(\lambda_j t)\int \exp(-\lambda_j s)\cdot\sum_{m=1}^{n} a_{jm}(s)x^q{}_m(s)\,ds$$
$$= \exp(\lambda_h t)n^q a^{q+1}(t)/[(q+1)!\gamma^{q+1}], \qquad j \neq h,$$

$$x^{q+1}{}_h(t) = \exp(\lambda_h t)[c^{q+1} + \int_0^t \exp(-\lambda_h s)\sum_{l=1}^{n} a_{lh}(s)x^q{}_l(s)\,ds]$$
$$= n^q \exp(\lambda_h t)a^{q+1}(t)/[(q+1)!\gamma^{q+1}].$$

In the case of $x^q{}_j(t)$, $j \neq h$, the limits of integration are established as previously stated. Here $a^{q+1}(t)$ is an a. p. function which again has no constant term and whose least frequency is greater than $(q+1)\gamma$. Since the $a_{ij}(t)$ are all a. p., there exists an M such that for all values of i, j, and t, $|a_{ij}(t)| < M$, from which it follows that $|a^{q+1}(t)| < (2M)^{q+1}/[(q+1)!\gamma^{q+1}]$. From this last inequality, we obtain $|x^{q+1}{}_h(t) \leqq \exp(\lambda_h t)[(2nM/\gamma)^{q+1}/(q+1)!]$. Thus for $x_h(t) = \sum_{q=0}^{\infty} x^q{}_h(t)$, we have the majorant $\exp(\lambda_h t + 2nM/\gamma)$, and for the series of a. p. functions which are multiplied by $\exp(\lambda_h t)$, we have the majorant $\exp(2nM/\gamma)$. By standard arguments, $x(t) = \sum_{q=0}^{\infty} x^q(t)$ is a solution of our equation. Since the uniform limit of a sequence of a. p. functions is again an a. p. function, the desired result follows in the case of simple roots. We next consider the case of multiple roots. For a solution corresponding to a given λ_k, of multiplicity $m+1$, the h-th component, corresponding to a root, $\lambda_j \neq \lambda_k$, has the basic integral

$$\exp(\lambda_j t) \int \exp(-\lambda_j s) s^m/m!\, a^q(s) \exp(\lambda_k s)(t-s)^h/h!\, a(s)\, ds.$$

Here we have $h \leqq r$, the maximum multiplicity of all the λ_j. Then integrating by parts, it follows that

$$\int_{\pm\infty}^{t} \exp[\lambda_j(t-s)](t-s)^h/h!\, a^q(s) s^m/m! \exp(\lambda_k s) a(s)\, ds$$
$$= \sum_{s=0}^{m} t^{m-s} a^{q+1}_s(t) \exp(\lambda_k t)/[(m-s)!(q\gamma)^{s+h+1}].$$

Thus, except for the fact that λ_j is a multiple root, so that now we may have up to r^2 terms and so that $\exp(2nMr^2/(\gamma) + \lambda_k t)$ is used instead of $\exp(2nM/(\gamma) + \lambda_k t)$ as a majorant, everything proceeds as before. In the case in which we are considering components $x^q{}_h(t)$ corresponding to λ_k, we obtain after integration by parts an expression of the form

$$\exp(\lambda_k t) \cdot \{ \sum_{i=0}^{m} t^{m-i} a^{q+1}(t)/[(m-i)!(q\gamma)^{i+h+1}] + \sum_{i=0}^{k} t^i a^{q+1}(0)/[i!(q\gamma)^{m+h+i}]\},$$

$(k \leqq m)$. Therefore, we choose, as in the case of simple roots, a set of initial coordinates for these components so as to cancel out the set of terms due to the lower limit (i. e. 0) of integration. As before, the convergence of the sum of these initial coordinates follows from the convergence arguments for the series itself. Now, except for this special choice of coordinates at $t = 0$ for certain components of $x^q(t)$, the argument proceeds as in the previous cases except that now the bound on our series is of the form

$$\exp(2nMn^2/(\gamma)+\lambda_k t)\sum_{i=0}^{m} t^{m-i}/(m-i)\,!.$$

This completes the proof of Theorem 2.

An immediate consequence of the above theorem and the work of Favard [6] is the following corollary.

COROLLARY. *If for the system $x'=A(t)x+B(t)$, where $B(t)$ is an* a. p. *vector and $A(t)$ satisfies the conditions of Theorem 2, the associated A_0 has roots all of whose real parts are nonzero, then this system has a unique* a. p. *solution.*

Part II. In this section, we consider the question of the existence of a. p. solutions for systems of the form $x'=A(t)x+B(t)$, where $A(t)$ is an $n\times n$ matrix and $B(t)$ an n vector of a. p. functions (Theorem 3). Before considering the statement of the theorem and its proof, it will be convenient to introduce several definitions for systems of the form $x'=[A+C(t)]x+B(t)$. Let $\lambda_j=\alpha_j+i\eta_j$, $j=1,\cdots,h$, denote the characteristic roots of A, $m=\min|\alpha_j|$, and p be the number of λ_j that are conjugate roots of A. From now on, we assume that the parameters have been changed so that $m\geqq 1$, and we denote the multiplicity of λ_j by m_j. If c denotes $\operatorname{l.u.b.}_{t,i,j}|c_{ij}(t)|$, then the system $x'=[A+C(t)]x+B(t)$ is said to satisfy the inequality I if for some $\epsilon>0$, one has $m-\epsilon>c\sum_{j=1}^{h}(p+m_j)(m_j)^2$. The statement of Theorem 3 now takes the following form.

THEOREM 3. *Consider the system $x'=(A+C(t))x+B(t)$, where $B(t)$ and $C(t)$ have real* a. p. *entries. If this system satisfies inequality I, defined above, then it possesses a unique* a. p. *solution whose module is contained in the module of $[C(t),B(t),\mathrm{Im}(\lambda_j)]$.*

Proof. We first consider the case in which A has simple roots. We assume a solution of the form $x(t)=x^0(t)+\sum_{i=1}^{\infty}x^i(t)$, where the $x^i(t)$ are defined recursively as follows: $[x^0(t)]'=Ax^0(t)+B(t)$ and $[x^i(t)]'=Ax^i(t)+C(t)x^{i-1}(t)$ for $i>0$. For convenience, we assume that $\mathrm{Re}(\lambda_i)>0$ for $i>j$ and $\mathrm{Re}(\lambda_i)<0$ for $i\leqq j$. In the formula for the variation of constants for the i-th components, we choose the limit of integration as ∞ $(-\infty)$ if $i>j$ $(i\leqq j)$. Thus, if we denote by k the $\operatorname{l.u.b.}_{\text{all } l}|B_l(t)|$, we have for the i-th component of $x^0(t)$, $x^0{}_i(t)=\int_t^{\infty}\exp(\lambda_h(t-s))B_h(s)\,ds$;

hence $|x^0{}_i(t)| \leqq k/m$. In the case of a conjugate root λ_l, we have for the k-th component $\int_t^\infty \exp[\lambda_l(t-s)][B_k(s)\cos\eta_k(t-s)+B_{k+1}(s)\sin\eta_l(t-s)]\,ds$. Thus the componentwise bound now takes the form $|x^0{}_k(t)| \leqq 2k/m$. For the induction step, we assume

$$\text{[a]} \qquad \|x^{l-1}(t)\| \leqq [k(n+p)/m]\cdot[((n+p)c)/m]^{l-1};$$

then by the formula for variation of constants,

$$\text{[b]} \qquad |x^l{}_s(t)| \leqq [kc(n+p)/m][((n+p)c/m]^{l-1},$$

or

$$\text{[c]} \qquad |x^l{}_s(t)| \leqq [2kc(n+p)/m][((n+p)c)/m]^{l-1}$$

in the case of a conjugate root. Thus

$$\text{[d]} \qquad \|x^l(t)\| \leqq [k(n+p)/m][(n+p)c/m]^l,$$

and the induction is complete. By assumption, $(n+p)c/m=\delta<1$, and the series for $x(t)$ is majorized by

$$[(n+p)k/m][1+\delta+\cdot\cdot\cdot]=(n+p)k/[m(1-\delta)]$$

and so converges uniformly. By Lemma 1, the $x^l(t)$ are a. p. and their modules are contained in the module described in the theorem. Since the uniform limit of a. p. functions is again a. p., the proof of the theorem is complete in the case of distinct roots. In the case of multiple roots, the procedure is exactly the same except that now one employs Lemma 1′ and uses the fact that $m>1$, so that $|k|/m^l<|k|/m$ for any integer l. Then if $J=\sum_{j=1}^{h}(m_j+p)(m_j)^2/m$, the estimates [a], [b], [c], and [d] take the form

$$\text{[a′]} \qquad \|x^{l-1}(t)\| \leqq kJ(Jc)^{l-1},$$

$$\text{[b′]} \qquad |x^l{}_s(t)| \leqq kJ(Jc)^{l-1}c(m_j)^2,$$

$$\text{[c′]} \qquad |x^l{}_s(t)| \leqq 2kJ(Jc)^{l-1}c(m_j)^2,$$

$$\text{[d′]} \qquad \|x^l(t)\| \leqq kJ(Jc)^l,$$

and the proof proceeds as in the case of simple roots. This completes the proof of Theorem 3.

The above result introduces the following problem. Given a matrix $B(t)$, is it possible to find a constant matrix A such that, if δ denotes the l. u. b. $|a_{ij}-b_{ij}(t)|$, then the inequality I′) $m-\epsilon>\delta\sum_{j=1}^{h}(p+m_j)(m_j)^2$ holds

for some positive ϵ, where p and m_j are as in Theorem 3? The matrix that immediately suggests itself is $A^0 = (a^0_{ij})$, where

$$a^0_{ij} = [\text{l.u.b.}\, a_{ij}(t) + \text{g.l.b.}\, a_{ij}(t)]/2,$$

since this will minimize the δ which will be multiplied by at least n. Thus we have:

COROLLARY. *If the roots* λ_j *of the equation* $x^n + a^0_{n-1}x^{n-1} + \cdots + a^0_0 = 0$ *associated with the system* $x^{(n)} + p_{n-1}(t)x^{(n-1)} + \cdots + p_0(t) = Q(t)$ *have nonzero real parts and if* $\min|\operatorname{Re}\lambda_j|$ *satisfies the inequality* I′ *above, the system has a unique* a. p. *solution.*

UNIVERSITY OF KANSAS.

REFERENCES.

[1] A. S. Besicovitch, *Almost Periodic Functions,* Cambridge University Press, 1932.

[2] S. Bochner, "Homogeneous systems of differential equations with almost periodic coefficients," *Journal of the London Mathematical Society,* vol. 8 (1933), pp. 283-288.

[3] H. Bohr, *Almost Periodic Functions,* Chelsea Publishing Company, New York, 1947.

[4] R. Cameron, "Systems of linear differential equations with almost periodic coefficients," *Acta Mathematica,* vol. 68 (1938), pp. 21-56.

[5] S. Diliberto, "On systems of ordinary differential equations," Contributions to the theory of nonlinear oscillations, *Annals of Mathematics Studies Number 20,* 1950.

[6] J. Favard, "Sur les equations differentielles linear a coefficients presque-periodique," *Acta Mathematica,* vol. 51 (1928), pp. 31-81.

[7] J. Lillo, "On almost periodic solutions of differential equations," to appear in the *Annals of Mathematics.*

[8] L. Markus, "Continuous matrices and the stability of differential systems," *Mathematische Zeitschrift,* vol. 62 (1955), pp. 310-319.

[9] F. Murray, "On certain linear differential equations of second order," *Annals of Mathematics,* vol. 24 (1922), pp. 69-88.

[10] O. Perron, "Uber eine Matrixtransformation," *Mathematische Zeitschrift,* vol. 36 (1936), pp. 465-473.

[11] S. Sandor, "Sur les equation differentielles linearies d'order superieur aux coefficients presques periodiques," Academia Republicie Populare Romîne. Buletin Stiintific. Secţiunea de stii ţe Matematice şi Fizice (1955), pp. 329, 346.

[12] A. Wintner and C. Putnam, "Linear differential equations with a. p. or Laplace transform coefficients," *American Journal of Mathematics,* vol. 73 (1951), pp. 792-806.

TAME COVERINGS AND FUNDAMENTAL GROUPS OF ALGEBRAIC VARIETIES.*

Part I: Branch loci with normal crossings; Applications: Theorems of Zariski and Picard.

By Shreeram Abhyankar.

Introduction. In this paper, we shall study the fundamental group of an algebraic variety V minus a subvariety W over an arbitrary ground field, the classical case being subsumed as a special case. This will be done via first studying finite alegbraic coverings of V with branch loci contained in W. Here in the introduction, we shall only approximately describe the situation and indicate some of the results.

The finite galois groups over V of all tame (for definition see Section 2) finite galois coverings of V—isomorphic coverings being identified—with branch loci contained in W form an inverse system $\pi'(V-W)$ of a special kind which we shall call a group tower. A group G is said to be a weak parent group of a group tower π if G can be topologized so that the group tower of all continuous finite homomorphic images of G is isomorphic to π; if π is isomorphic to the group tower of *all* finite homomorphic images of G (i. e. if G is regarded as a discrete group), then G is said to be a parent group of π.[1] The possible existence of a finitely generated parent group (or somewhat weaker: the possible existence of a finitely generated weak parent group) of $\pi'(V-W)$ is the abstract analogue of the statement (Section 16) that in the classical case the topological fundamental group $\pi_1(V-W)$ is finitely generated; and hence if such a finitely generated parent (respectively, weak parent) group exists, we shall call it a tame fundamental parent (respectively, weak parent) group of $V-W$. Now one main result of this paper (Section 12) is that if V is nonsingular and simply connected, if W has only normal crossings and if the irreducible components of W move in linear systems of dimension greater than one, then denoting the number of these

* Received April 23, 1958.

[1] Here we chose to overlook a condition that the intersection of subgroups of G of finite index be 1, see Section 5; and for the corresponding situation in the classical case, see Section 17.

components by t, we have that $V - W$ has a tame fundamental weak parent group generated by t generators and that *any* tame fundamental weak parent group (and hence, in particular, any tame fundamental parent group) of $V - W$ is t-step nilpotent and is abelian in case the irreducible components of W are pairwise connected, i. e. any two have a point in common. As a corollary of this, we deduce the abstract version of a theorem of Zariski which in the classical case says that the fundamental group of a complex projective space minus a hyperplane with normal crossings and t irreducible components is an abelian group with t generators and one relation. As another corollary, we deduce the abstract version of a theorem of Picard which says that any 'cyclic' surface in the complex projective three space is simply connected.

Now in the classical case, the recent work of Grauert and Remmert shows that any finite unramified topological covering of $V - W$ can be completed to an alegbraic covering of V with branch locus contained in W, and hence $\pi_1(V - W)$ is a parent group of $\pi'(V - W)$. Therefore the above results tell us that in the classical case, $\pi_1(V - W)$ is respectively t-step nilpotent, and abelian.[1]

Our tools are mainly these: (1) Galois theory of local rings, including the concepts of splitting and inertia groups which are the higher dimensional analogues of the corresponding concepts in algebraic number theory and are due to Krull. These and other aspects of the galois theory of local rings were further developed by us in our previous work. In Section 2, we bring together, in suitable form, concepts and results to be used from this theory. (2) From algebraic geometry proper, we use mainly three things all due to Zariski, namely (i) normalization in an algebraic extension, (ii) generalized Bertini theorem, and (iii) degeneration principle. (3) Results from the local theory of normal crossings developed by us elsewhere and summarized in Section 3; this in part is the arithmetization of local fundamental groups; in our previous treatment of this, we had used Zariski's theorem on 'purity of branch locus,' while in our forthcoming new treatment which makes the theory valid also in the Kroneckerian case, we shall use Chow's recent work on 'connectedness' and 'local Bertini theorem.' (4) From topology, we derive our motivation for the fundamental group tower, etc. All these tools put together enable us to study fundamental groups in the abstract case when no classical topological techniques are available.

In forthcoming papers, we shall study fundamental groups of algebraic varieties when the branch loci have higher singularities, and there, in addition to the present tools, we shall employ analysis of singularities, quadratic trans-

formations and a concept of systems of curves with assigned singularities; and as an application, we shall obtain theorems on the nonexistence of irreducible plane curves of a given degree with prescribed singularities. Also in another paper, we shall develop a 'ramification theory' for complex manifolds and obtain similar results for fundamental groups of complex manifolds; in that set up, the role played in the algebrogeometric situation by the generalized Bertini theorem and the degeneration principle will be played by a result of Stein and a result of Serre.

For the sake of brevity, definiteness and clarity of exposition, in this paper, we shall deal with algebraically closed ground fields and projective varieties. That most of the relevant material of this paper goes over for nonalgebraically closed ground fields or for the complete abstract varieties of Weil will be shown in a later communication.

The contents of the various chapters and sections should be clear from their titles.

In concluding this introduction, I wish to express my great appreciation of Professor Oscar Zariski; for in the first place, the present investigations began in trying to carry over to the abstract case Zariski's classical theorem on fundamental groups mentioned above; and in the second place, as indicated, some of the important tools in this study are due to Zariski's foundations of abstract algebraic geometry.

TABLE OF CONTENTS

A. Algebrogeometric Preliminaries.

1. Conventions and notations. A ring R (always commutative with identity) will be said to be normal if it is integrally closed in its total ring of quotients. By "(R, M) is a local ring," we shall mean that R is a (not necessarily noetherian) local ring and M is its maximal ideal. Let (R, M) be a normal local ring with quotient field K, let K^* be a finite separable algebraic extension of K; recall that the integral closure of R in K^* has only a finite number of maximal ideals, the quotient rings with respect to these maximal ideals will be called the *local rings in K^* lying above R*; if (R^*, M^*) is a local ring in K^* lying above (R, M), then $R = K \cap R^*$ and $M = K \cap M^*$, and hence we may call (R, M) the local ring in K lying below (R^*, M^*); also recall that if K^*/K is galois, then the set of local rings in K^* lying above R is a complete set of K-conjugates. A field extension K^*/K will be said to be galois if it is normal algebraic and separable; $G(K^*/K)$ will then denote the galois group of K^*/K; unless otherwise stated, galois will mean finite galois. As usual, for a finite alegbraic extension K^*/K, $[K^*:K]_s$ and $[K^*:K]_i$ denote, respectively, the separable and the pure inseparable degrees of K^*/K. For a subgroup H of a group G, the index of H in G will be denoted by $[G:H]$; in particular, $[G:1]$ is the order of G.

Let V be an irreducible algebraic variety in a projective space over an algebraically closed ground field k and let $K = k(V)$, i.e. let K/k be a function field of V/k; then V is a projective model of K/k and is given by projectively related affine coordinate rings with quotient field K/k. Unless otherwise stated, we shall consider only those irreducible subvarieties (respectively, points) of V which are defined (respectively, rational) over k, thus the irreducible subvarieties of V will be in one to one correspondence with the quotient rings of the various affine coordinate rings of V in K/k. For an irreducible subvariety W of V, we shall denote the local ring of W on V by $Q(W, V)$, and the maximal ideal of $Q(W, V)$ by $M(W, V)$; note that k is a subfield of $Q(W, V)$ and K is the quotient field of $Q(W, V)$. V will be said to be normal if the local ring of each point (and hence, of each irreducible subvariety) of V is normal. Unless otherwise stated, terms like 'connected,' etc. will refer to the Zariski topology (over the ground field under consideration).

2. Galois theory of local rings and branch loci. In this section, we shall collect together, in suitable form, concepts and results on galois theory of local rings and branch loci. These will be based on Section 2 of [A2],[2]

[2] References in square brackets refer to the References at the end of the paper.

Section 1 of [A1], Sections 1, 5 and 6 of [A3], and when proofs are not given, they will be found in these references.

Let K^*/K be a galois extension, let (R, M) be a normal local ring with quotient field K and let (R^*, M^*) be a local ring in K^* lying above R. Recall that

$G_s(R^*/R) = G_s(R^*/K) =$ *splitting group* of R^* over R (or K) $=$ group of automorphisms t of K^*/K for which $t(R^*) = R^*$.

$G_i(R^*/R) = G_i(R^*/K) =$ *inertia group of* R^* over R (or K) $=$ group of automorphisms t of K^*/K for which $r \in R^*$ implies that $t(r) - r \in M^*$.

The fixed fields of $G_s(R^*/R)$ and $G_i(R^*/R)$ are respectively called the *splitting* and *inertia fields* of R^* over R (or of R^* over K).

LEMMA 1. *Let* $G = G(K^*/K)$, $G_s = G_s(R^*/R)$, $G_i = G_i(R^*/R)$. *Then*

(i) $[G : G_s] =$ *number of local rings in* K^* *lying above* R.

(ii) G_i *is a normal subgroup of* G_s *and* $[G_s : G_i] = [R^*/M^* : R/M]_s$.

(iii) $[G_i : 1] = [K^* : K]$ [number of local rings in K^* lying above $R]^{-1}[R^*/M^* : R/M]_s^{-1}$.

LEMMA 2. *Let* K' *be a subfield of* K^* *which is galois over* K, *and let* (R', M') *be a local ring in* K' *lying above* (R, M) *such that* R^* *lies above* R'. *Then* (i) *the natural homomorphism of* $G(K^*/K)$ *onto* $G(K'/K)$ *induces a homomorphism of* $G_s(R^*/R)$ *onto* $G_s(R'/R)$ *with kernel* $G_s(R^*/R')$ *and a homomorphism of* $G_i(R^*/R)$ *onto* $G_i(R'/R)$ *with kernel* $G_i(R^*/R')$. *Hence in particular:*

(ii) $$[G_s(R^*/R) : 1] = [G_s(R^*/R') : 1][G_s(R'/R) : 1] \text{ and}$$
$$[G_i(R^*/R) : 1] = [G_i(R^*/R') : 1][G_i(R'/R) : 1].$$

Proof. (i) follows from a straightforward application of galois theory in view of the equations: $R' = R^* \cap K'$ and $M' = M^* \cap K'$. (ii) follows from (i), and can also be proved directly thus: Since $[K^* : K] = [K^* : K'][K' : K]$; $[R^*/M^* : R/M]_s = [R^*/M^* : R'/M']_s[R'/M' : R/M]_s$; and the local rings in K^* lying above R are exactly the local rings in K^* lying above the various local rings in K' which lie above R; in view of Lemma 1, it is enough to show that if $\bar{R}^*$ is any local ring in K^* lying above R and $\bar{R}' = \bar{R}^* \cap K'$, then $G_s(\bar{R}^*/\bar{R}')$ and $G_i(\bar{R}^*/\bar{R}')$ are of the same orders, respectively, as $G_s(R^*/R')$ and $G_i(R^*/R')$. Since R^* and $\bar{R}^*$ are K-conjugate, there exists $t \in G(K^*/K)$

with $t(R^*) = \bar{R}^*$. Let u be an element of $G(K^*/K')$ considered as a subgroup of $G(K^*/K)$. Then $g \in G_s(\bar{R}^*/\bar{R}')$ if and only if $g(\bar{R}) = \bar{R}^*$, i.e., $g(t(R^*)) = t(R^*)$, i.e., $(t^{-1}gt)(R^*) = R^*$, i.e., if and only if $t^{-1}gt \in G_s(R^*/R')$. Hence $G_s(\bar{R}^*/R')$ and $G_s(R^*/R')$ are conjugate in G, and similarly for the inertia groups.

LEMMA 3. *Let $K_1, K_2, \cdots, K_t$ be subfields of K^* such that K^* is their compositum and each of them is galois over K. Let R_j be a local ring in K_j lying above R. Then $G_i(R^*/R)$ is isomorphic to a subgroup of the direct sum of $G_i(R_1/R), G_i(R_2/R), \cdots, G_i(R_t/R)$ whose natural projection on each of the components $G_i(R_j/R)$ is onto; hence, in particular, for each j, the order of $G_i(R_j/R)$ divides the order of $G_i(R^*/R)$ and the latter divides the product of the orders of $G_i(R_1/R), \cdots, G_i(R_t/R)$. Similar statements hold for the splitting groups.*

Proof. Apply inductions on t and use Lemma 2 repeatedly.

Now let K be an algebraic function field over an algebraically closed field k of characteristic p, let K^* be a finite separable algebraic extension of K, let V be a normal projective model of K/k, let V^* be a K^*-normalization of V and let ϕ be the natural map of V^* onto V. Recall that V^* is characterized, up to natural biregular maps, by the property that for any irreducible subvariety W of V, if $W^*_1, \cdots, W^*_t$ denote the irreducible components of $\phi^{-1}(W)$, then $Q(W^*_1, V^*), \cdots, Q(W^*_t, V^*)$ are exactly the local rings in K^* lying above $Q(W, V)$. Concepts and adjectives defined for $Q(W^*_j, V)$ over $Q(W, V)$ will be applied to W^*_j over V (or over K); thus, for instance, if K^*/K is galois, then the inertia group of $Q(W^*_j, V)$ over $Q(W, V)$ will be called the inertia group of W^*_j over V or over K and will be denoted by $G_i(W^*_j/V)$ or $G_i(W^*_j/K)$. Strictly speaking, these concepts depend on the particular rational map ϕ of V^* onto V, i.e. on the particular embedding of $k(V)$ into $k(V^*)$; however, this will be always clear from the context.[3]

Let W^* be an irreducible subvariety of V^*, let $W = \phi(W^*)$, let (R^*, M^*) and (R, M) be the completions, respectively, of $Q(W^*, V^*)$ and $Q(W, V)$ canonically assuming that R is a subring of R^*, let E^* and E be the quotient

[3] For visual and mental facility, by an abuse of language, when the reference to V is clear from the context and there is no cause for confusion, we shall allow ourself to apply concepts and adjectives for W^*_j over V as if they were for W^*_j over W; thus, for instance, we may write $G_i(W^*_j/W)$ for $G_i(W^*_j/V)$, or we may call $r(W^*: V)$ the ramification index of W^* over W and denote it by $r(W^*: W)$. [Note that if U^* is an irreducible subvariety of V^* containing W^* and $U = \phi(U^*)$, then $r(W^*/W)$ will in general depend on whether this is over U or V].

fields of R^* and R respectively, let E' be a least galois extension of E containing E^*, and let R' be the integral closure of R in E'. Since R is complete, R' is a local ring and the only one in E' lying above R; let M' be the maximal ideal in R'. We set

$$r(W^*:V) = \textit{ramification index of } W^* \textit{ over } V \ (\textit{or over } K)$$
$$= [E^*:E][R^*/M^*:R/M]_s^{-1}.^3$$

We shall say that W^* is *ramified for* ϕ (or over V, or over K) if $r(W^*:V) \neq 1$, i.e., $r(W^*:V) > 1$, and we shall say that W^* is tamely ramified for ϕ (or over V, or over K) if

$$[E':E][R'/M':R/M]_s^{-1} \not\equiv 0 \ (\mathrm{mod}\, p)$$

in case $p \neq 0$ (and no restriction if $p = 0$).[4] W will be said to be *ramified* for ϕ^{-1} (or for V^*, or in K^* since this is independent of the model V^*) if some irreducible component of $\phi^{-1}(W)$ is ramified for ϕ. Again, W will be said to be *tamely ramified* for ϕ^{-1} (or for V^*, or in K^*) if each irreducible component of $\phi^{-1}(W)$ is tamely ramified for ϕ. If each irreducible subvariety of V is tamely ramified in K^*, then K^* will be said to be a *tamely ramified extension of* V, or *tamely ramified over* V, or V^* will be said to be *a tamely ramified covering of* V. The set of points of V which are ramified in K^* will be called *the branch locus of* V *in* K^* or the branch locus of K^* (or V^*) over V, or the branch locus of ϕ^{-1} and *will be denoted by* $\Delta(K^*/V)$ or $\Delta(V^*/V)$. Since k is algebraically closed, $\Delta(K^*/V)$ is the set of points P of V for which $\phi^{-1}(P)$ consists of less than $[K^*:K]$ points. If $\Delta(K^*/V)$ is empty, then we shall say that K^* *is unramified over* V or that V^* *is an unramified covering of* V.

LEMMA 4. *$\Delta(K^*/V)$ is a proper subvariety of V, and an irreducible subvariety of V is ramified in K^* if and only if it is contained in $\Delta(K^*/V)$.*

Now let K' be a least galois extension of K containing K and let W' be an irreducible subvariety corresponding to W on a K'-normalization V' of V.

LEMMA 5. $\Delta(K'/V) = \Delta(K^*/V)$.

---

[4] In [A3], we have defined 'tamely ramified' to mean $r(W^*: V) \not\equiv 0 \ (\mathrm{mod}\, p)$. As was shown in Section 5 of [A3], these two definitions coincide for curves (over an algebraically closed ground field). However, for higher dimensional varieties, the definition given in [A3] is not the correct one and the present definition should be substituted in [A3]; for otherwise, Remark 9 of Section 9 of [A3], which is the generalization of Theorem 5 there to higher dimensional varieties, need not be true. Also note that 'tamely ramified' includes 'unramifield.'

Invoking Lemma 5 of Section 2 of [A2], Lemma 1 of Section 5 of [A3], and Lemmas 1, 3, and 5 of this section, we get the following two lemmas.

LEMMA 6. $r(W':W)=[G_i(W'/W):1]$; *hence W is ramified in K' if and only if $[G_i(W'/W):1]\neq 1$, and W is tamely ramified in K' if and only if $[G_i(W'/W):1]\not\equiv 0 \pmod p$ in case $p\neq 0$ (and trivially always for $p=0$).*

LEMMA 7. *W is tamely ramified in K' if and only if W is tamely ramified in K^*.*

Hence 'ramified' and 'tamely ramified' for an irreducible subvariety of V can be defined without passing to completions of the local rings. Also for galois extensions K'/K, 'ramification index,' 'ramified,' and 'tamely ramified' can be defined for irreducible subvarieties of V as well as those of V' without passing to completions of the local rings.

LEMMA 8. *Let $K\subset K_1\subset K_2$ be finite separable algebraic extensions and let V_1 be the K_1-normalizations of V. If K_1/V is tamely ramified and K_2/V_1 is tamely ramified, then K_2/V_1 is tamely ramified.*

Proof. Use Lemma 4 of Section 2 of [A2].

LEMMA 9. *Let K^* and K_1 be finite separable algebraic extensions of K and let K^*_1 be a compositum of K^* and K_1. Let V^* be a K^*-normalization of V. If K_1/V is unramified (respectively, tamely ramified), then K^*_1/V^* is unramified (respectively, tamely ramified).*

Proof. In view of Lemmas 5 and 7, we may assume K^*/K, K_1/K and K^*_1/K are galois. Let W^*_1 be an irreducible subvariety on a K^*_1-normalization of V and let W, W^* and W_1 be the corresponding irreducible subvarieties of V, V^*, and a K_1-normalization of V. Then by Lemmas 3 and 6, we have that $r(W^*_1:W)$ divides $r(W^*:W)r(W_1:W)$, and by Lemma 4 of Section 2 of [A2], we have that $r(W^*_1:W)=r(W^*_1:W^*)r(W^*:W)$. Therefore $r(W^*_1:W^*)$ divides $r(W_1:W)$.

Part of Lemma 6 of Section 2 of [A2] is this:

LEMMA 10. *Let $U'\subset W'$ be irreducible subvarieties of V'. Then $G_s(W'/V)\subset G_s(U'/V)$ and $G_i(W'/V)\subset G_i(U'/V)$.*

Lemmas 7 and 10 give the following:

LEMMA 11. *K^*/V is tamely ramified if and only if each point of V is tamely ramified in K^*.*

Lemmas 2, 3 and 7 give the following lemma.

LEMMA 12. *Let* $K_1 \subset K_2$ *and also* $L_1, L_2, \cdots, L_h$ *be finite separable algebraic extensions of* K *and let* L *be a compositum of* $L_1, L_2, \cdots, L_h$. *Let* D *be a subvariety of* V. *Then*

(1) $\Delta(K_2/V) \subset D$ *implies* $\Delta(K_1/V) \subset D$; *and* $\Delta(L_j/V) \subset D$ *for* $j = 1, \cdots, h$ *implies* $\Delta(L/V) \subset D$. *Also,* (2) K_2 *is tamely ramified over* V *implies* K_1 *is tamely ramified over* V; *and* L_j *is tamely ramified over* V *for* $j = 1, \cdots, h$ *implies* L *is tamely ramified over* V.

Lemmas 4 and 5 of Section 2 of [A2] imply the following:

LEMMA 13. *Let* K_1 *be a field contained between* K *and the inertia field of* W' *over* W, *and let* W_1 *be the irreducible subvariety corresponding to* W' *on a* K_1*-normalization of* V. *Then* W_1 *is unramified over* V.

Since a one dimensional normal local domain is a discrete valuation ring, we have

LEMMA 14. *If* W' *is an irreducible subvariety of* V' *of codimension* 1 *and if* K' *is tamely ramified over* V, *then* $G_i(W'/V)$ *is cyclic and its order is prime to* p *in case* $p \neq 0$.

Let v be a real valuation of K/k and let v' be a K'-extension of v. By $G_s(v'/v) = G_s(v'/K)$ and by $G_i(v'/v) = G_i(v'/K)$, we shall denote, respectively, the *splitting* and *inertia groups* over K of the valuation ring of v'. We shall say that v is *ramified* in K' if $G_i(v'/v) \neq 1$, also, we shall say that v is tamely ramified in K' if $[G_i(v'/v):1] \not\equiv 0 \pmod{p}$ in case $p \neq 0$, (since K'/K is galois, this does not depend on v'). Then a part of Lemma 6 of Section 2 of [A2] gives

LEMMA 15. *If* K' *is unramified over* V, *then every real valuation of* K/k *is unramified in* K'. *If* K' *is tamely ramified over* V, *then every real valuation of* K/k *is tamely ramified in* K'.

Zariski's theorem on 'purity of branch locus' says the following:

LEMMA 16. *If* P *is a simple point of* V, *then at* P, $\Delta(K^*/V)$ *is of codimension* 1 (*and hence of pure codimension* 1).

The proof of this given in [A1, Theorem 1] is incorrect. Professor Zariski has a correct proof (to be published), and we have a proof of the following weaker form which will be published in [A5].

LEMMA 17. *If P is a simple point of V and if P is tamely ramified in K^*, then at P, $\Delta(K^*/U)$ is of codimension* 1 *(and hence of pure codimension* 1*).*

Lemma 16 will not be used in this paper except for an incidental observation in Section 10 (Lemma 30).

3. Local theory of normal crossings. Let (R, M) be the local ring of a simple point P on an irreducible n dimensional algebraic variety V, let W be a subvariety of V which is pure $n-1$ dimensional at P and let $W_1, W_2, \cdots, W_t$ be the irreducible components of W passing through P. Let q_j and q be the ideals at P, respectively, of W_j and W; i.e., $q_j = R \cap M(W_j, V)$ and $q = q_1 \cap q_2 \cap \cdots \cap q_t$. Let $(\bar{R}, \bar{M})$ be a completion of (R, M). We shall say that W has an *h-fold normal crossing at P* if there exists a minimal basis $x_1, x_2, \cdots, x_n$ of $\bar{M}$ such that

$$q_1\bar{R} = x_1 x_2 \cdots x_{u_1}\bar{R}, \qquad q_2\bar{R} = x_{u_1+1}x_{u_1+2}\cdots x_{u_2}\bar{R}, \cdots,$$
$$q_t\bar{R} = x_{u_{t-1}+1}x_{u_{t-1}+2}\cdots x_{u_t}\bar{R}; \text{ with } 0 < u_1 < u_2 < \cdots < u_t = h. \qquad \cdots\cdots (A).$$

It is clear that the index h is uniquely determined by W at P, i.e., it is independent of the basis $x_1, \cdots, x_n$. Note that $\bar{R}$ is a unique factorization domain, and hence each q_j is a principal ideal and q is also equal to $q_1 q_2 \cdots q_t$. We assert that W has an h-fold normal crossing at P if and only if any one of the following conditions holds: (1) There exists a minimal basis $x_1, \cdots, x_n$ of $\bar{M}$ with $x_{h+1}, x_{h+2}, \cdots, x_n$ in R such that we have (A) with $\bar{R}$ replaced by R. (2) There exists a basis $x_1, \cdots, x_n$ of $\bar{M}$ with $x_{h+1}, x_{h+2}, \cdots, x_n$ in R such that $q = x_1 x_2 \cdots x_h R$. (3) There exist elements $x_{h+1}, x_{h+2}, \cdots, x_n$ in R such that $q x_{h+1} x_{h+2} \cdots x_n \bar{R}$ is generated by the product of the elements in some minimal basis of $\bar{M}$. For assume that there exists a minimal basis $x_1, \cdots, x_n$ of $\bar{M}$ such that (A) holds. Fix v_j in R with $v_j R = q_j$ for $j = 1, \cdots, t$. Then the generator of $q_j\bar{R}$ exhibited in (A) differs from v_j by a multiplicative unit in $\bar{R}$, and hence by multiplying $x_1, \cdots, x_h$ by suitable units in $\bar{R}$, we may assume that the generators of $q_j\bar{R}$ exhibited in (A) coincides with v_j for $j = 1, 2, \cdots, t$. Now there exists y_j in R with $y_j \equiv x_j \pmod{\bar{M}}$. Then $x_1, x_2, \cdots, x_h, y_{h+1}, y_{h+2}, \cdots, y_n$ is also a minimal basis of $\bar{M}$, and hence we could assume that x_j is in R for $j = h+1, h+2, \cdots, n$; this gives (1), and (2) and (3) at once follow from (1). Now we shall prove the converse. (1) trivially implies that W has an h-fold normal crossing at P. That (2) and (3) imply that W has an h-fold normal crossing at P follows from the

fact that $\bar{R}$ is a unique factorization domain and that the elements of any minimal basis of $\bar{M}$ are mutually prime irreducible nonunits of $\bar{R}$.

W will be said to have *a strong h-fold normal crossing at P* if in (A), we have $u_1 = u_2 - u_1 = u_3 - u_2 = \cdots = u_t - u_{t-1} = 1$ and hence $t = h$. In view of conditions (1) and (2) above, this is equivalent to saying that there exists a minimal basis $x_1, x_2, \cdots, x_n$ of M such that

$$(1^*) \quad q_j = x_j R \text{ for } j = 1, 2, \cdots, t = h; \qquad \text{or} \quad (2^*) \quad q = x_1 x_2 \cdots x_h R.$$

Geometrically speaking, W has a normal crossing at P if P is a simple point of each analytic sheet of W and the tangent hyperplanes to these sheets at P are linearly independent; if the number of sheet is h, then the normal crossing is h-fold. Furthermore, the normal crossing is strong if P is a simple point for each algebraic component of W so that at P, the number of algebraic components of W is equal to the number of analytic sheets of W. Also note that what we called a normal crossing in [A1] is now being called a strong normal crossing.

Now let K be an n dimensional algebraic function field over an algebraically closed ground field k of characteristic p, let K^* be a galois extension of K, let V be a normal projective model of K/k, let V^* be a K^*-normalization of V, let ϕ be the rational map of V^* onto V, let P^* be a point of V^*, let $P = \phi(P^*)$; assume that P is a simple point of V, that P is tamely ramified in K^* and that $\Delta(K^*/V)$ has a normal crossing at P. Observe that since k is algebraically closed, we have that $G_i(P^*/P) = G_s(P^*/P)$. Now we assert the following:

PROPOSITION 1. *$G_i(P^*/P)$ is abelian.*

From Proposition 1, one can deduce the following:

PROPOSITION 2. *Let W be an irreducible component of $\Delta(K^*/V)$ through P. Then W does not split (locally) at P^*,* i. e., *only one irreducible component of $\phi^{-1}(W)$ passes through P^*.*

Now Proposition 1, in case of strongly normal crossings, was proved in Theorem 2 of [A], the proof there was based on 'purity of branch locus,' i. e., Lemma 16 or Theorem 1 of [A1], or in fact, only on 'purity of branch locus for tame coverings,' i. e., Lemma 17. The proof of Theorem 1 of [A1] is incorrect. For not necessarily strong normal crossings, one could adapt the proof of [A1], provided one has 'purity' also for algebroid varieties. Professor Zariski's new proof (unpublished) of 'purity' is believed to be also applicable for the algebroid case. However, in a forthcoming paper [A5],

we shall prove Proposition 1 and 2 directly (and simultaneously), deriving 'purity' (for tame coverings) as an incidental corollary; the treatment there will be applicable to algebraic, algebroid, as well as Kroneckerian varieties; in that treatment, we shall use Chow's recent work on 'connectedness' and 'local Bertini theorem' [C2, 3]. Here we shall briefly indicate the idea of how, for strong normal crossings, one can deduce Proposition 2 from Proposition 1. Let then $W = W_1, W_2, \cdots, W_h$ be the irreducible components of $\Delta(K^*/V)$ at P; let (R, M) be the local ring of P on V; choose a minimal basis $x_1, \cdots, x_n$ of M such that x_jR is the ideal of W_j at P. If the assertion is proved for an algebraic extension of K^*, then it will *a fortiori* imply it for K^*, and hence we may replace K^* by a suitable algebraic extension. Making considerations as in Section 2 of [A1], Proposition 1 will imply that (extending K^* suitably) we may arrange matters so that the completions of $Q(P^*, V^*)$ and $Q(P, V)$ are, respectively,

$$\bar{R}^* = k[[x_1{}^{1/m}, x_2{}^{1/m}, \cdots, x_h{}^{1/m}, x_{h+1}, x_{h+2}, \cdots, x_n]]$$

and $\bar{R} = k[[x_1, x_2, \cdots, x_n]]$, where $m \not\equiv 0 \pmod{p}$ in case $p \neq 0$.[5] The matter being 'local,' we may replace K^*/K by E^*/E, where E^* and E are the quotient fields of $\bar{R}^*$ and $\bar{R}$ respectively. Now it is enough to observe that $x_1\bar{R}^*$ is prime, or rather that the valuation v_1 given by $x_1\bar{R}$ does not split in E^*; for instance, because in E^*, v_1 is ramified to index m and acquires a separable residue field extension of degree $(h-1)m$.

We remark that Proposition 1, in the classical case, follows from the fact that the local topological fundamental group at a normal crossing is abelian.

4. Linear systems. In this section, we recall needed information on linear systems [Z4, 6]. Let K be an n dimensional algebraic function field over an algebraically closed ground field k and let V be a normal projective model of K/k. We shall use the notations and definitions of Section 2 of [Z6] with the following modification: (1) an $(n-1)$ cycle on V will be called a divisor; (2) we shall not operate in a universal domain, but shall operate within K/k, i.e., all the divisors (unless otherwise stated) will be rational over k, all the functions will be in K and so on. Let us, for instance, recall that for a positive divisor D on V, $|D|$ *denotes the complete linear system determined by* D, it is the linear system of all nonnegative divisors on V which are linearly equivalent to D, and we have

[5] Actually, in [A1], the procedure was reversed, i.e., first it was shown that R^* and R can be arranged thus, and from it, the abelian character of $G_i(P^*/P)$ was deduced.

$$\dim |D| = [k\text{-dimension of the vector space of all functions } f \text{ in } K \text{ for which } (f) + D \geqq 0] - 1.$$

Part of the considerations of [Z4], especially Sections 14 and 15, can be stated in the following form:

"GENERALIZED THEOREM OF BERTINI." *Let L be a linear system free from fixed components and of dimension greater than* 1. *If L is composite with a pencil, i. e., if the rational map given by L maps V onto a curve, then each member of L is irreducible, and conversely, if L is not composite with a pencil, i. e., if the rational map given by L maps V onto a variety of dimension greater than* 1, *then L contains an irreducible member, or equivalently, a "generic" member of L is absolutely irreducible (here we are going outside our ground field k).*

Note that if D is a prime divisor with $\dim |D| \geqq 1$, *then $|D|$ is without fixed components.* Now let K^* be a finite separable algebraic extension of K, let V^* be a K^*-normalization of V, and let ϕ be the rational map of V^* onto V. Let L be a linear system on V without fixed components and of dimension greater than 1. Given D in L, write $D = m_1D_1 + \cdots + m_tD_t$, where the D_j are prime divisors and $m_j > 0$; let $D_{j1}, D_{j2}, \cdots, D_{jq_j}$ be the irreducible components of $\phi^{-1}(D_j)$; set $D^* = \sum_{j=1}^{t} m_j \sum_{h=1}^{q_j} r(D_{jh}:D_j)D_{jh}$; and let L^* be the set of divisors D^* on V^* spanned out as D ranges over L. Then it is easily verified that L^* is a linear system on V^* without fixed components and that the rational map of V^* given by L^* is the compositum of ϕ and the rational map of V given by L; hence L^* is composite with a pencil if and only if L is composite with a pencil. *We* shall denote the linear system L^* *by $\phi^{-1}(L)$ and shall call it the ϕ^{-1} image of L.*

B. Preliminaries on Group Towers.

5. Definitions. Let us recall the definition of an inverse system of groups [ES, Chapter VIII]: A *partially ordered set* S is a set with a relation $s < t$ which is transitive and reflexive such that $s < t$ and $t < s$ in S implies that $s = t$. A *directed set* S is a partially ordered set such that s, t in S implies that there exists u in S with $s < u$ and $t < u$. Let S' be a (partially ordered) subset of a directed set S; S' will be said to be a *cofinal subset* of S if s in S implies that there exists s' in S' with $s < s'$; S' will be said to be a *saturated subset* of S if $s < s'$ in S with s' in S' implies that s is in S'; note

that if S' is a saturated subset of S and S'' is a subset of S', then S'' is a saturated subset of S' if and only if S'' is a saturated subset of S, also if S' is a saturated and cofinal subset of S then S' must be S itself. An inverse system π *of groups* is a set $\{G_s\}$ of groups indexed by s running over a directed set S, together with homomorphisms $\alpha_s{}^t\colon G_t \to G_s$ for each $s < t$ in S, such that $\alpha_s{}^s =$ identity for s in S and $\alpha_s{}^t \alpha_t{}^u = \alpha_s{}^u$ for $s < t < u$ in S. If S' is a directed subset of S, the corresponding groups $\{G_s\}$ with s in S' form a *subsystem* π' of π; π' will be said to be a *cofinal* (*respectively: saturated*) *subsystem* of π if S' is a cofinal (respectively: saturated) subset of S'. Sometimes we shall take the set $\{G_s\}$ of groups as it own indexing set.

Let G be a group; let S be the set of all normal subgroups $s, t, \cdots$ of G with the relation $s < t$ if and only if $s \supset t$, now the intersection of any two normal subgroups is again a normal subgroup, and hence *S is a directed set*; when we talk of a partially ordered (in particular, directed) set S' of normal subgroups of a group G, we shall always be referring to this order relation; S' will be said to be a *saturated* (*respectively: directed, cofinal*) *set of normal subgroups of G* if S' is a saturated (respectively: directed, cofinal) subset of S. Let G be a group and let S' be a directed set of normal subgroups of G; by G/S', we shall denote the family of factor groups $\{G/s'\}$ of G indexed by s' running over S' and together with the natural onto homomorphisms; G/S' is then clearly an inverse system of groups; let S be the set of all normal subgroups of G, we shall call G/S *the derived inverse ysstem of G*; now G/S' is a subsystem of G/S, and it is a saturated (respectively: cofinal) subsystem if and only if S' is a saturated (respectively: cofinal) subset of S.

Let π be an inverse system of finite groups. Then π will be called a *group tower* if for each G_t in π, the inverse subsystem of π consisting of all G_s with $s < t$ is isomorphic to the derived inverse system of G_t under an isomorphism which is the identity on G_t. Observe that a subsystem of a group tower is a subtower if and only if it is a caturated subsystem; also note that a group tower has no cofinal subtowers other than itself. Now let G be a group, then the subset of all finite groups of the derived inverse system of G is a saturated subsystem [6] and it will be called the derived group tower of G; note that if S' is a set of normal subgroups of G, then G/S' is a group tower if and only if S' is a saturated set of normal subgroups of finite indices. If π is a group tower and p is a prime number, then the group in π

[6] (i) Any subgroup containing a subgroup of finite index is again of finite index. (ii) From the isomorphism theorem, it follows that the intersection u of any two normal subgroups s and t of finite indices is again of finite index; in fact, the index of u divides the product of the indices of s and t.

of G of finite index, let π be a group tower, and observe the following: (A′) there exists a normal subgroup M of G such that G/M is a weak parent group of π if and only if there exists a set S of normal subgroups of G such that G/S is isomorphic to π. [*'If'*: Set M = the intersection of all groups in S. *'Only if'*: G/M is a weak parent group of π implies that there exists a set S^* of normal subgroups of G/M such that $(G/M)/S^*$ is isomorphic to π and the intersection of all the groups in S^* is 1; let S be the set of all $\phi^{-1}(s^*)$ with s^* in S^*, where ϕ is the canonical homomorphism of G onto G/M.] (B') G/N is a parent group of π if and only if π is isomorphic to the derived group tower of G. (C′) G/N is a modulo p quasi parent group of π if and only if there exists a subtower π' of the derived group tower of G such that π' contains the modulo p derived group tower of G, and π' is isomorphic to π. (D′) G/N is a modulo p parent group of π if and only if there exists a subtower π' of the derived group tower of G, such that π' contains the modulo p derived group tower of G, the intersection of "the kernels in G of the various groups in π'" is 1, and π' is isomorphic to π.

6. Topological considerations for group towers. In this section, we wish to make some incidental observations which easily follow from well known general facts [P, Chapter III; ES, Chapter VIII]. All topological groups considered will be assumed to be Hausdorff.

Remark 1. Let G be a group which is the weak parent group of some group tower, i.e., there exists a saturated set S of normal subgroups of G of finite index such that the intersection of all the groups in S is 1. Then G can be topologized by considering the members of S as a system of neighborhoods of the identity, and then S will coincide with the set of *closed* normal subgroups of G of finite index so that G/S will exactly be the group tower of all *continuous* finite homomorphic images of G. Conversely, if G is a topological group such that the intersection of all closed normal subgroups of G of finite index is 1, then G/S is a group tower, where S is the set of all closed normal subgroups of G of finite index. Thus we could give the following equivalent definition of weak parent groups (and call it a *topological parent group*): *A weak parent group of a group tower π is a topological group G in which the intersection of all closed normal subgroups of finite index is* 1 (*or equivalently the intersection of all closed subgroups of finite index is* 1) *such that π is isomorphic to the group tower of all continuous finite homomorphic images of G.* Note that such a group G must be totally disconnected, and also observe that for a topological group G, a sub-

group of finite index is closed if and only if it is open. *If G is to be a parent group, then the topology must be the one—or any other stronger than the one—obtained by taking for a system of neighborhoods of the identity all subgroups of finite index.*

Remark 2. Let $\pi = \{G_s, \alpha_s{}^t, s \in S\}$ be a group tower and let G_∞ be the inverse limit of π. Recall that G_∞ is the subgroup of $\prod_{s \in S} G_s$ consisting of elements $x = \{x_s\}$ for which $\alpha_s{}^t(x_t) = x_s$ for all $s < t$ in S. If we consider the G_s to be discrete topological groups, G_∞ becomes a compact group. G_∞ is a weak parent group of π since in G_∞, the intersection of closed normal subgroups of finite index is 1 and π is canonically isomorphic to the derived tower of continuous finite homomorphic images of G_∞. Let G' be any weak parent group of π with a weak parent map f of G' onto π and kernel S'. For g in G', set $\phi(g) = \{x_{f(s')}\}$, where $x_{f(s')} = f_{s'}(g)$. Then ϕ is easily seen to be an isomorphism of G' into G_∞. If we topologize G' by considering members of S as a system of neighborhoods of the identity, then ϕ is continuous and $\phi(G')$ is dense in G_∞. Conversely, a subgroup of G_∞ is dense if and only if the restriction of the natural projections of G_∞ into G_s maps G' onto G_s for all s in S, i.e., if and only if these projections give an isomorphism between π and the group tower of all continuous finite homomorphic images of G' thus making G' a weak parent group of π. Hence (up to a topological isomorphism) G_∞ is the only *compact "topological" parent group* of π.

Remark 3. Now assume that π is a group tower indexed by a countable set. Then the topologized inverse limit of π is compact totally disconnected and satisfies the second axiom of countability. Conversely, a compact totally disconnected topological group satisfying the second axiom of countability is canonically topologically isomorphic to the topologized inverse limit of its topological group tower (i.e., the group tower of continuous finite homomorphic images).

7. Existence of weak parent groups, parent groups, etc.

Example 1. Eilenberg and Zippin have communicated the following example which shows that in a topological compact totally disconnected group satisfying the second axiom of countability, a subgroup of finite index need not be closed; and in view of Remark 3 of Section 6, this shows that *the inverse limit of a group tower need not be its parent group under the natural map.* Let G be the product of countably infinite copies of a group Z_2 with

two elements 0 and 1. Considering Z_2 to be discrete, G then becomes compact totally disconnected and satisfies the second axiom of countability. Let G' be the corresponding direct sum considered as a subgroup of G. Then G' is dense in G. There exist subgroups H of G of index two containing G' and hence not closed in G. For instance, (i) consider Z_2 as a field and treat G as a vector space over Z_2, then any subgroup of G is a vector subspace and since $\dim G/G'$ is not zero (in fact is infinite), there are lots of subspaces H of G containing G' with $\dim(G/H) = 1$; or (ii) fix x in G not in G' and let H be a maximal element in the set of subgroups of G containing G' but not x.

Example 2. Let H be an infinite cyclic group, and let π be the modulo p derived group tower of H for a given prime number p; then it is clear that *H is a finitely generated weak parent group of π and hence a finitely generated modulo p parent group of π.* Suppose, if possible, that π has a finitely generated parent group G. Then (Proposition 4 of Section 9) G must be abelian. Since π contains a group of any order prime to p, it is clear that G cannot be finite. Hence G can be mapped homomorphically onto an infinite cyclic group and hence onto a finite cyclic group of any order including p. Therefore G cannot be a parent group of π. *Thus π has no finitely generated parent group.*

Remark 4. Note that the inverse limit G of a group tower π cannot be finitely generated unless G is finite, i. e., unless π contains only a finite number of groups. For since G is a compact topological group, G has a non-trivial left invariant Haar measure such that the measure of G is a non-zero positive real number, and since this measure is countably additive, it follows that G cannot be countable unless it is finite.

8. Finitely generated group towers.

Definition. A group tower $\pi = \{G_s, \alpha_s^t, s \in S\}$ will be said to be finitely generated if there exists an integer n such that each G_s is generated by n elements; we shall then say that π is generated by n generators. A family $\{(s_1, s_2, \cdots, s_n), s \in S\}$ will be said to be *a consistent family of n-generators of π* if for each s in S, $(s_1, s_2, \cdots, s_n)$ are generators of G_s and for each $s < t$ in S, $\alpha_s^t(t_j) = s_j$ for $j = 1, 2, \cdots, n$. Note that if a cofinal subset of π has a consistent family of n generators, then it can uniquely be extended to a consistent family of n generators of π. If π has a consistent family of n generators, then π *will be said to be consistently generated by n generators.*

LEMMA 18. *Let G be a finitely generated group and let m be a given integer. Then G contains only a finite number of subgroups of index m.*

Proof. Since any subgroup of G of index m contains a normal subgroup of G of index which is a factor of $m!$ (= the order of the symmetric group on m letters),[7] it is enough to prove our assertion for normal subgroups of G. Let $x_1, x_2, \cdots, x_n$ be a set of generators of G. Let S_m be the symmetric group on m letters. A homomorphism of G into S_m is uniquely determined by giving the images of $x_1, x_2, \cdots, x_n$, and for each x_j, there are at most $m!$ possible choices, hence the number q of distinct homomorphisms of G into S_m is finite, namely, $q \leqq (m!)^n$. For a normal subgroup N of G of index m, let f_N denote the canonical homomorphism of G onto G/N. Since any group of order m is isomorphic to a subgroup of S_m, we can fix an isomorphism g_N of G/N into S_m; set $h_N = g_N f_N$. Then h_N is a homomorphism of G into S_m and $h_N^{-1}(1) = N$. Therefore distinct normal subgroups N of G of index m give rise to distinct homomorphisms of G into S_n. Hence the number of such subgroups is $\leqq q$ and hence finite.

LEMMA 19. *Let $\pi = \{G_s, \alpha_s^t, s \in S\}$ be a finitely generated group tower. Then for any given integer m, there are only a finite number of G_s of order m.*

Proof. Suppose π is generated by n generators and let F_n be the free group on m generators. By Lemma 18, there are only a finite number q of normal subgroups of F_n of index m. Suppose, if possible, that there are more than q groups in π of order m, choose $q+1$ of them, say $G_{s1}, G_{s2}, \cdots, G_{sq+1}$. Since S is directed, there exists s in S with $s > sj$ for $j = 1, 2, \cdots, q+1$. Let f be a homomorphism of F_n onto G_s and let $f_j = \alpha_{sj}^s f$. Since π is a tower, the kernels of $\alpha_{s1}^s, \alpha_{s2}^s, \cdots, \alpha_{sq+1}^s$ are all distinct, and hence the kernels of $f_1, f_2, \cdots, f_{q+1}$ are all distinct; since these are all normal subgroups of F_n of index m, this is a contradiction.

LEMMA 20. *Let S be a countable directed set. Then S contains an ascending cofinal sequence $s_1 < s_2 < \cdots$.*

Proof. If S is finite,it is enough to take $s_1 = s_2 = \cdots =$ *the* maximum of S. Now assume S is not finite and let $n_1, n_2, \cdots$ be a counting up of S. Let $s_1 = u_1$, choose s_2 with $s_2 > s_1$ and $s_2 > u_2$, choose s_3 with $s_3 > s_2$ and $s_3 > u_3, \cdots$, etc.

LEMMA 21. *Let $\pi = \{G_s, s \in S\}$ be a group tower. Assume that there are only a finite number of groups G_s of any given order. Then S contains a cofinal ascending sequence.*

Proof. The assumption implies that S is countable. Now apply Lemma 20.

PROPOSITION 3. *Let $\pi = \{G_s, s \in S\}$ be a finitely generated group tower. Then S contains a cofinal ascending sequence.*

Proof. Follows from Lemmas 19 and 21.

LEMMA 22. *Let $\pi = \{G_s, \alpha_s{}^t, s \in S\}$ be a group tower. Then the following three conditions are equivalent: (1) π is consistently generated by n generators; (2) π has a weak parent group generated by n generators; (3) π is isomorphic to a subtower of the derived group tower of a group generated by n generators. Furthermore, if $\{(s_1, s_2, \cdots, s_n), s \in S\}$ is a consistent family of n generators of π, then there exists a group G generated by n generators $a_1, a_2, \cdots, a_n$, and a weak parent map $g = \{g_s \colon G \to G_s, s \in S\}$ of G onto π such that $g_s(a_j) = s_j$ for all s in S and $j = 1, 2, \cdots, n$; G is unique in the sense that if H is any other group generated by n generators $b_1, b_2, \cdots, b_n$ with a weak parent map $h = \{h_s \colon H \to G_s, s \in S\}$ such that $h_s(b_j) = s_j$ for all s in S and $j = 1, 2, \cdots, n$, then there exists a (unique) isomorphism of G onto H with $a_j \to b_j$ for $j = 1, 2, \cdots, n$.*

Proof. It is obvious that (2) implies (3); also (3) implies that there exists a group P with n generators and a family p of homomorphisms of P onto the various G_s consistent with the maps $\alpha_s{}^t$; if Q is the intersection of the kernels of all the members of p, then P/Q is a weak parent group of π and is generated by n generators, which implies (2); again it is obvious that (3) implies (1). Now assume (1) and let $\{(s_1, s_2, \cdots, s_n), s \in S\}$ be a consistent family of n generators of π. Let F_n be the free group on n generators $x_1, x_2, \cdots x_n$, and let f_s be the homomorphism of F_n onto G_s given by $f_s(x_j) = s_j$. Let $M = \bigcap_{s \in S} f_s{}^{-1}(1)$, let u be the canonical homomorphism of F_n onto $G = F_n/M$ and let $a_j = u(x_j)$. Since $M \subset f_s{}^{-1}(1)$, there exists a unique homomorphism g_s of G onto G_s with $f_s = g_s u$. Then $g = \{g_s, s \in S\}$ is a weak parent map of G onto π with $g_s(a_j) = s_j$ for s in S and $j = 1, 2, \cdots, n$. Now let $H, b_1, b_2, \cdots, b_n, h$ be as stated. Since F_n is free, there exists a unique homomorphism v of F_n onto H with $v(x_j) = b_j$ for $j = 1, 2, \cdots, n$. Then $h_s v(x_j) = s_j$, and hence $h_s v = f_s$ for all s in S, and hence $v^{-1}(1) \bigcap_{s \in S} f_s{}^{-1}(1)$. Also $d \in F_n$, $d \notin u^{-1}(1)$ implies that $v(d) \neq 1$, which, in view of the assumption that h is a weak parent map, implies that $f_s(d) = h_s(v(d)) \neq 1$, i.e., $d \notin f_s{}^{-1}(1)$. Hence $v^{-1}(1) \supset \bigcap_{s \in S} f_s{}^{-1}(1)$. Therefore $v^{-1}(1) = \bigcap_{s \in S} f_s{}^{-1}(1) = M$, and hence vu^{-1} is an isomorphism of G onto H with $a_j \to b_j$ for $j = 1, 2, \cdots, n$.

Now let G be a group generated by t generators $a_1, a_2, \cdots, a_t$ such that a_1 generates a normal subgroup A_1 in $G_1 = G$, a_2 generates a normal subgroup A_2 in $G_2 = G_1/A_1$, a_3 generates a normal subgroup A_3 in $G_3 = G_2/A_2$, $\cdots, a_{t-1}$ generates a normal subgroup A_{t-1} in $G_{t-1} = G_{t-2}/A_{t-2}$, and a_t generates $A_t = G_t = G_{t-1}/A_{t-1}$.

For a normal subgroup H of G, let f_H denote the canonical homomorphism of G onto $G_H = G/H$. Then it is clear that G_H has the same property as G with respect to th sequence $f_H(a_1), f_H(a_2), \cdots, f_H(a_t)$; also it is clear that the groups which now correspond to $G_1, G_2, \cdots, G_t$, $A_1, A_2, \cdots, A_t$ are the canonical images of these under f_H, i.e., in a natural way, they are $f_H(G_1)$, $f_H(G_2), \cdots, f_H(G_t)$, $f_H(A_1), f_H(A_2), \cdots, f_H(A_t)$. Note that *if the order of one of the a_j in G_j is finite, then it is divisible by the order of $f_H(a_j)$ in $f_H(G_j)$*. Also observe that *the order of $f_H(a_1)$ in G_H is simply the order of $A_1/(H \cap A_1)$, i.e., the order of a_1 in $A_1/(H \cap A_1)$*.

LEMMA 23. *Let $n_1, n_2, \cdots, n_t$ be given positive integers. Let S be the set of normal subgroups H of G such tat in $f_H(G_j)$ the order of $f_H(a_j)$ divides n_j for $j = 1, 2, \cdots, t$. Then for any subset S' of S, $\bigcap_{H \in S'} H$ is again in S.*

Proof. First observe that S is not empty since it contains G itself Let $K = \bigcap_{H \in S} H$. Now if K is in S, then any normal subgroup of G containing S is obviously again in S, and since the intersection of the members of any subset of S contains K, that intersection must lie in S. Hence it is enough to prove that K is in S. Now we shall make induction on t. For $t = 1$, G is cyclic, and hence K is the *unique* normal subgroup of G whose index is n_1 if G is infinite, and the greatest common divisor of n_1 and the order of G if G is finite. Next assume that $t > 1$ and that the lemma is true for $t - 1$. We have $K \cap A_1 = \bigcap_{H \in S} (H \cap A_1)$, and hence, applying the lemma to A_1, we conclude by the last italicized statement before the lemma that the order of a_1 in $f_K(G_1)$ is a factor of n_1. Next, let ϕ be the canonical homomorphism of $G = G_1$ onto $G_2 = G_1/A_1$. Then H in S implies that $\phi(H)$ satisfies the conditions of the lemma for G_2 with respect to $\phi(a_2), \phi(a_3), \cdots, \phi(a_t)$ and $n_2, n_3, \cdots, n_t$ respectively. Hence, applying the lemma for $t - 1$ to this and observing that $\phi(K) = \bigcap_{H \in S} \phi(H)$, we conclude that the orders of $f_K(a_2)$, $\cdots, f_K(a_t)$ in $f_K(G_2), \cdots, f_K(G_t)$ divide $n_2, \cdots, n_t$ respectively. Therefore K is in S.

LEMMA 24. (i) *Let $n_1, \cdots, n_t$ be given positive integers. Then there exists at most one normal subgroup K in G such that $f_K(a_j)$ is of order n_j*

in $f_K(G_j)$ *for* $j=1,\cdots,t$. (ii) *Now let* $m_1,\cdots,m_t$ *be another set of positive integers such that* m_j *divides* n_j *for* $j=1,\cdots,t$. *Assume that there exist normal subgroups* H *and* K *of* G *such that* $f_H(a_j)$ *and* $f_K(a_j)$ *are, respectively, of orders* m_j *and* n_j *in* $f_H(G_j)$ *and* $f_K(G_j)$ *for* $j=1,\cdots,t$. *Then* $H\supset K$.

Proof. (i) Let K and K_1 be two normal subgroups with the required property and let $K^*=K\cap K_1$. Then by Lemma 23, the order n^*_j of $f_{K^*}(a_j)$ in $f_{K^*}(G_j)$ divides n_j. Since $K^*\subset K$, $f_K(G)$ is canonically homomorphic to $f_{K^*}(G)$, and hence, by the last but one italicized statement before Lemma 23, n^*_j divides n_j. Therefore $n^*_j=n_j$. Since $G/K=f_K(G_1)\supset f_K(G_2)\supset\cdots\supset f_K(G_t)\supset 1$ is a normal sequence of G/K in which the orders of the successive factors are $n_1,\cdots,n_2$, the order of G/K must be $n_1n_2\cdots n_t$. Similarly, the order of G/K_1 is $n_1n_2\cdots n_t$ and the order of G/K^* is $n^*_1n^*_2\cdots n^*_t=n_1n_2\cdots n_t$. Since $K^*\subset K$ and $K^*\subset K_1$, this says that $K=K^*=K_1$.

(ii) Let $L=H\cap K$. Then by an argumnet similar to the one used in the proof of (i), we conclude that the order of G/L equals the order of G/K, and hence $L=K$, i.e., $H\supset K$.

9. Solvable, nilpotent and abelian group towers. [References: K1, Chapter IV and K2, Chapters XIV and XV.] Let G be a group. Recall that G is *solvable* means that G has a finite solvable normal series and G is *nilpotent* means that G has a finite central series. We shall say that G is *m-step* solvable if G has a solvable normal series of length m, and we shall say that G is *m-step nilpotent* if G has a central series of length m. In this section, for any group G, we shall denote by $D_q(G)$ and $E_q(G)$ subgroups of G defined by setting: $D_0(G)=E_0(G)=G$, $D_j(G)=$ the commutator subgroup of $D_{j-1}(G)$, $E_j(G)=$ the subgroup of G generated by the commutators of G and $E_{j-1}(G)$. It is well known that G is m-step solvable if and only if $D_m(G)=1$ and that G is m-step nilpotent if and only if $E_m(G)=1$; in particular, G is 1-step nilpotent if and only if G is abelian and G is 2-step nilpotent if and only if the commutator subgroup $D_1(G)$ of G is contained in the center of G. *We shall say that a group tower* π *is m-step solvable (respectively: m-step nilpotent, abelian) if and only if every group in* π *is m-step solvable (respectively: m-step nilpotent, abelian).*

LEMMA 25. *Let* $f\colon G\to H$ *be an onto homomorphism.* i *Then for all* j, *we have* $f(D_j(G))=D_j(H)$ *and* $f(E_j(G))=E_j(H)$.

Proof. It is obvious for D_0 and E_0; suppose $j>1$ and assume it is true for D_{j-1} and E_{j-1}. Now u in $D_j(G)$ implies that there exist a,b in $D_{j-1}(G)$

with $u = aba^{-1}b^{-1}$; then $f(u) = f(a)f(b)f(a)^{-1}f(b)^{-1}$ and this is in $D_j(H)$ since, by assumption, $f(a)$ and $f(b)$ are in $D_{j-1}(H)$; conversely, u^* in $D_j(H)$ implies that there exist a^*, b^* in $D_{j-1}(H)$ with $u = a^*b^*a^{*-1}b^{*-1}$; then, by assumption, there exist a, b in $D_{j-1}(G)$ with $f(a) = a^*$ and $f(b) = b^*$, hence $u = aba^{-1}b^{-1}$ is in $D_j(G)$ and $f(u) = u^*$. Again, u in $E_j(G)$ implies that there exist a in $E_{j-1}(G)$ and b in G with either $u = aba^{-1}b^{-1}$ or $u = bab^{-1}a^{-1}$; then, by assumption, $f(a)$ is in $E_{j-1}(H)$ and $f(u) = f(a)f(b)f(a)^{-1}f(b)^{-1}$ or $f(u) = f(b)f(a)f(b)^{-1}f(a)^{-1}$ respectively, so that, in either case, $f(u)$ is in $E_j(H)$; conversely, u^* in $E_j(H)$ implies $\cdots$, etc. The proof is complete by induction.

LEMMA 26. *Let G be a group and let S be a set of onto homomorphisms $s\colon G \to H_s$ of G such that $\bigcap_{s \in S} s^{-1}(1) = 1$. If there exists an integer m such that for all s in S, H_s is m-step solvable (respectively m-step nilpotent), then G is m-step solvable (respectively, m-step nilpotent). For a and b in G, if $s(a)$ and $s(b)$ commute for all s in S, then a and b commute; in particular, if H_s is abelian for all s in S, then G is abelian.*

Proof. Assume that H_s is m-step solvable for all s in S. Then by Lemma 25, for each s in S, we have $D_m(G) \subset s^{-1}(D_m(H_s)) = s^{-1}(1)$. Therefore $D_m(G) \subset \bigcap_{s \in S} s^{-1}(1) = 1$. Hence $D_m(G) = 1$, i.e., G is m-step solvable. The statement for 'm-step nilpotent' follows similarly. For a, b in G, if $s(a)$ and $s(b)$ commute for each s in S, then

$$aba^{-1}b^{-1} \in \bigcap_{s \in S} s^{-1}(1) = \{1\},$$

and hence a and b commute.

Specializing Lemma 26 to group towers, we may state:

PROPOSITION 4. *Let G be a weak parent group of a group tower π. Then G is m-step solvable (respectively: m-step nilpotent, abelian) if and only if π is m-step solvable (respectively: m-step nilpotent, abelian) if and only if every weak parent group of π is m-step solvable (respectively: m-step nilpotent, abelian). For a, b in G, a and b commute if and only if their images (under a given weak parent map of G onto π) in every member of π commute.*

LEMMA 27. *In a finitely generated abelian G, the intersection of subgroups of finite index is 1, i.e., G is a parent group of its derived group tower.*

Proof. G is a direct product of cyclic subgroups $G_1, G_2, \cdots, G_n$; *let* f_j be the projection of G onto G_j. We want to show that $g \in G$, $g \neq 1$ implies

that there exists a homomorphism ϕ of G onto a finite group such that g is not mapped onto the identity. Now $g \neq 1$ implies that $f_j(g) \neq 1$ for some j, hence we may replace G by G_j, i. e., we may assume that G is cyclic. If G is finite, we may take ϕ to be the identity isomorphism of G onto G. If G is infinite, let a be a generator of G and let $g = a^u$, let n be a positive integer which does not divide u, let H be a cyclic group of order n with generator b and define ϕ by taking $\phi(a) = b$.

LEMMA 28. *Let G be a group which is generated by t subgroups $H_1, H_2, \cdots, H_t$ such that H_j is abelian and is normal in G. Then G is t-step nilpotent.*

Proof. First observe that if A and B are two normal subgroups in a group C and C is generated by A and B, then denoting the centers of A, B, C by $Z(A)$, $Z(B)$, $Z(C)$ respectively, we have that $Z(A) \cap Z(B) \subset Z(C)$. For the assumption implies that $C = AB$, i. e., every element $c \in C$ is of the form $c = ab$ with $a \in A$ and $b \in B$. Now $u \in Z(A) \cap Z(B)$ implies that $uc = uab = aub = abu = cu$, i. e., $u \in Z(C)$.

The above statement together with a trivial induction shows that the center $Z(G)$ of G contains the intersection of the centers of $H_1, H_2, \cdots, H_t$; since each H_j is abelian, it is its own center and hence $Z(G) \supset H_1 \cap H_2 \cap \cdots \cap H_t$.

Now we shall prove the lemma by induction on t. For $t = 1$, G is abelian and hence 1-step nilpotent; now suppose $t > 1$ and assume the lemma for $t - 1$. Let f_j be the canonical homomorphism of G onto G/H_j. Since G/H_j is generated by the $t-1$ subgroups $H_k/(H_j \cap H_k)$ $(k \neq j)$ each of which is abelian and normal in G/H_j, by the induction hypothesis, we conclude that $E_{t-1}(G/H_j) = 1$. By Lemma 25, we have

$$E_{t-1}(G) \subset \bigcap_{j=1}^{t} f_j^{-1}(E_{t-1}(G/H_j)) = \bigcap_{j=1}^{t} f_j^{-1}(1) = \bigcap_{j=1}^{t} H_j \subset Z(G).$$

Hence $E_t(G) = 1$.

10. Algebraic fundamental groups. Let K be an n dimensional algebraic function field over an algebraically closed ground field k of characteristic p and let Λ be a fixed alegbraic closure of K. Let V be a normal projective model of K/k and let W be a proper subvariety of V. Then as in Section 4 of [A3], we define:

[8] The notions here will be much more refined than those introduced in Section 4 of [A3]; note that fixing an algebraic closure Λ does not affect the notions of that section.

$\Omega(V-W)=$ the family of finite separable algebraic extensions L of K in Λ for which $\Delta(L/V)\subset W$.

$\Omega_g(V-W)=$ the family of members L of $\Omega(V-W)$ such that L/K is galois.

$\Omega'_g(V-W)=$ the family of members L of $\Omega_g(V-W)$ such that L/V is tamely ramified.

$\Omega^*_g(V-W)=$ the family of members L of $\Omega_g(V-W)$ such that $[L:K]\not\equiv 0 \pmod p$ in case $p\neq 0$ (and no restriction if $p=0$).

The galois groups over K of the members of $\Omega_g(V-W)$, or $\Omega'_g(V-W)$, or $\Omega^*_g(V-W)$ form, under the natural homomorphisms, group towers (Lemma 12, Section 2). We set

$\pi(V-W)=$ *the fundamental group tower of* $V-W$
$=$ the group tower of galois groups over K members of $\Omega_g(V-W)$.

$\pi'(V-W)=$ the *tame fundamental group tower* of $V-W$
$=$ the group tower of galois groups over K members of $\Omega'_g(V-W)$.

$\pi^*(V-W)=$ the *reduced fundamental group tower of* $V-W$
$=$ the group tower of galois groups over K members of $\Omega^*_g(V-W)$.

For brevity, sometimes we shall omit the adjective 'fundamental' from the above group towers.[9] Note that $\pi^*(V-W)$ is a subtower of $\pi'(V-W)$ which itself is a subtower of $\pi(V-W)$; if $p\neq 0$, then $\pi^*(V-W)$ consists exactly of those groups of $\pi(V-W)$ whose orders are prime to p, while if $p=0$, then $\pi^*(V-W)=\pi'(V-W)=\pi(V-W)$.

We shall say that $V-W$ is respectively: (1) *simply connected,* (2) *tamely simply connected,* or (3) *reduced simply connected*; according as: (1*) $\pi(V-W)=1$ (i.e., consists of the trivial group alone), (2*) $\pi'(V-W)=1$, or (3*) $\pi^*(V-W)=1$. It follows (Lemmas 5 and 7 of Section 2) that $V-W$ is simply connected (respectively: tamely simply connected) if and only if there does not exist any finite separable algebraic extension K^* of K ($K^*\neq K$, K^*/K not necessarily galois) for which $\Delta(K^*/K)\subset W$ (respec-

[9] Changing the algebraic closure Λ of K will affect these group towers only up to canonical isomorphisms.

tively: $\Delta(K^*/K) \subset W$ and K^*/V tamely ramified). We note the following trivial lemma.

LEMMA 29. (i) $\pi(V-W)=1$, $\pi'(V-W)=1$, $\pi^*(V-W)$ *respectively imply that* $\pi(V)=1$, $\pi'(V)=1$, $\pi^*(V)=1$. (ii) $\pi(V)=\pi'(V)$ *so that, in particular, V is simply connected if and only if V is tamely simply connected if and only if there does not exist any finite separable algebraic extension K^*/K ($K^* \neq K$, K^*/K not necessarily galois) such that K^*/V is unramified.*

Also we have the following:

LEMMA 30. *If V_1 and V_2 are two nonsigular projective models of K/k, then $\pi(V_1)=\pi(V_2)$, i.e., the fundamental group tower is a birational invariant for nonsingular projective models.*

Proof. Let K^*/K be a galois extension. Lemmas 15 and 16 of Section 2 imply that K^*/V is unramified if and only if each valuation of K/k is unramified in K^*.

LEMMA 31. *If V_1 and V_2 are two nonsigular projective models of K/k, then $\pi^*(V_1)=\pi^*(V_2)$ [so that $\pi(V_1)=\pi(V_2)$ in case $p=0$], i.e., the reduced fundamental group tower (and hence the fundamental group tower in case $p=0$) is a birational invariant for nonsingular projective models.*

Proof. This is a corollary of Lemma 30 and also follows from Lemmas 15 and 17 (Section 2).

Remark 5. Note that in the classical case when the ground field is the field of complex numbers, a stronger assertion can be made, namely, it is well known that the topological fundamental group is a birational invariant for nonsingular projective models.

Let G be a group. Then G will, respectively, be said to be (1) an *unrestricted fundamental weak parent group of* $V-W$, (1′) *an unrestricted tame fundamental weak parent group of* $V-W$, (1*) *an unrestricted reduced fundamental weak parent group of* $V-W$ if G is a weak parent group, respectively, of $\pi(V-W)$, $\pi'(V-W)$, $\pi^*(V-W)$. Secondly, G will, respectively, be said to be (2) *an unrestricted fundamental parent group of* $V-W$, (2′) *an unrestricted tame fundamental parent group of* $V-W$, (2*) *an unrestricted reduced fundamental parent* group of $V-W$ if G is a parent group, respectively, of $\pi(V-W)$, $\pi'(V-W)$, $\pi^*(V-W)$. Thirdly, G will, respectively, be said to be (3′) *a tame fundamental weak parent group*

of $V - W$, and (3*) *a reduced fundamental weak parent group* of $V - W$ if G is *finitely generated* and if G is a weak parent group, respectively, of $\pi'(V - W)$ and $\pi^*(V - W)$.

Next, G will be said to be (4′) *a tame fundamental parent* group of $V - W$ if G is *finitely generated* and G is a parent group of $\pi(V - W)$ $\pi'(V - W) = \pi^*(V - W)$ in case $p = 0$, while G is a modulo p parent group of $\pi'(V - W)$ in case $p \neq 0$. Finally, G will be said to be (4*) *a reduced fundamental parent group of* $V - W$ if G is *finitely generated* and G is a parent group of $\pi(V - W) = \pi'(V - W) = \pi^*(V - W)$ in case $p = 0$, while G is a modulo p parent group of $\pi^*(V - W)$ in case $p \neq 0$.

The adjectives 'fundamental' and 'group' from all the above objects may be omitted for brevity. Observe that for $p = 0$, the adjectives 'tame' and 'reduced' are superfluous.

Remark 6. Proposition 4 of Section 9 tells us that if one restricted tame fundamental weak parent group of $V - M$ is t-step solvable (respectively: t-step nilpotent, abelian), then so is any other unrestricted tame fundamental weak parent group of $V - W$ and hence, any tame fundamental parent group of $V - W$, etc.

Remark 7. The galois groups over K of the compositums, respectively, of $\Omega_g(V - W)$, $\Omega'_g(V - W)$ and $\Omega^*_g(V - W)$ are naturally isomorphic to the inverse limits, respectively, of $\pi(V - W)$, $\pi'(V - W)$ and $\pi^*(V - W)$, and hence they are, respectively, an unrestricted fundamental weak parent group of $V - W$, an unrestricted tame fundamental weak parent group of $V - W$ and an unrestricted reduced fundamental weak parent group of $V - W$. In connection with the existence of unrestricted parent groups, see Example 1 and Remark 4 of Section 7. For further discussion of the definitions of this section, see Section 16.

C. Main Results.

Throughout the rest of the paper, k will denote an algebraically closed field of characteristic p.

11. Finite coverings. Let V be a nonsingular projective n dimensional algebraic variety over k, let $K = k(V)$, let K^* be a finite separable algebraic extension of K, let V^* be a K^*-normalization of V, and let ϕ be the rational map of V^* onto V.

PROPOSITION 5. *If W is an irreducible $n-1$ dimensional subvariety of V such that* $\dim |W| > 1$, *then* $\phi^{-1}(W)$ *is connected.*

Proof. Since $\dim |W| > 1$ and W is irreducible, it follows by the generalized theorem of Bertini (Section 4) that $|W|$ is not composite with a pencil. Therefore $\phi^{-1}(|W|)$ is not composite with a pencil, and hence, again by the generalized theorem of Bertini, a 'general' member of $\phi^{-1}(W)$ is irreducible. Therefore by Zariski's degeneration principle [Z5, see also C1], (the support of) every member of $\phi^{-1}(|W|)$ is connected. Since $\phi^{-1}(W)$ is the support of the divisor in $\phi^{-1}(|W|)$ corresponding to W, we conclude that $\phi^{-1}(W)$ is connected.

PROPOSITION 6. *Now suppose that K^*/V is tamely ramified. Let W be a pure $n-1$ dimensional subvariety of V, with $W_1, W_2, \cdots, W_t$ as its distinct irreducible components, such that $\Delta(K^*/V) \subset W$. Assume that:* (1) $\dim |W_j| > 1$ *for* $j = 1, 2, \cdots, t$; *and* (2) *W has only normal crossings.*[10] *Then $\phi^{-1}(W_j)$ is irreducible for $j = 1, 2, \cdots, t$.*

Proof. Let K' be a least galois extension of K containing K^*; then K'/V is tamely ramified and $\Delta(K'/V) \subset W$ (Lemmas 5 and 7, Section 2), and if the 'inverse image' of W_j on the K'-normalization were irreducible, then $\phi^{-1}(W_j)$ would *a fortiori* would be irreducible; therefore we may assume that K^*/K is galois to begin with. By Proposition 5, $\phi^{-1}(W_j)$ is connected. Suppose, if possible, that $\phi^{-1}(W_j)$ is reducible; then at least two distinct irreducible components of $\phi^{-1}(W_j)$ must have a point P^* in common. Let $P = \phi(P^*)$. Now W_j is an irreducible component of $\Delta(K^*/V)$ and W has a normal crossing at P implies that $\Delta(K^*/V)$ has a normal crossing at P; therefore, by Proposition 2 (Section 4), only one irreducible component of $\phi^{-1}(W_j)$ passes through P^*. This is a contradiction, and hence the proposition is proved.

THEOREM 1. *Let K be an n dimensional algebraic function field over an algebraically closed ground field k of characteristic p, let V be a non-singular projective model of K/k, let W be a pure $n-1$ dimensional subvariety of V with distinct irreducible components $W_1, W_2, \cdots, W_t$. Let K^*/K be a galois extension such that K^*/V is tamely ramified and $\Delta(K^*/V) \subset W$. Let V^* be a K^*-normalization of V and let ϕ be the rational map of V^* onto V.*
Assume that:

[10] I. e., W has a normal crossing at each of its points.

(1) $\dim |W_j| > 1$ *for* $j = 1, 2, \cdots, t$;

(2) W *has only normal crossings; and*

(3) V *is simply connected.*

Then:

(A) $W^*_j = \phi^{-1}(W_j)$ *is irreducible for* $j = 1, 2, \cdots, t$.

(B) *The inertia group* $G_i(W^*_j/W_j)$ *is a cyclic normal subgroup (of order prime to* p *in case* $p \neq 0$) *of* $G(K^*/K)$ *for* $j = 1, 2, \cdots, t$. *Let* a_j *be a generator of* $G_i(W^*_j/W_j)$.

(C) $G(K^*/K)$ *is generated by* $G_i(W^*_1/W_1), G_i(W^*_2/W_2), \cdots, G_i(W^*_t/W_t)$, *Hence*

(D) $G(K^*/K)$ *is generated by the* t *generators* $a_1, a_2, \cdots, a_t$ *each of which generates a normal subgroup.*

(E) $G(K^*/K)$ *is* t*-step nilpotent and its order is not divisible by* p *in case* $p \neq 0$.

(F) *If* W_j *and* W_k *have a point in common, then* a_j *and* a_k *commute in* $G(K^*/K)$.

(G) *If* $W_1, W_2, \cdots, W_t$ *are pairwise connected, i.e., any two have a point in common, then* $G(K^*/K)$ *is abelian.*

Proof. (A) follows from Proposition 6. Hence we can talk of $G_i(W^*_j/W_j)$; since $Q(W_j, V)$ does not split in K^*, $G_s(W^*_j/W_j) = G(K^*/K)$, and hence (B) follows from Lemmas 1 and 14 of Section 2. Now let H be the subgroup of $G(K^*/K)$ generated by $a_1, a_2, \cdots, a_t$ and let K_1 be the fixed field of H. Then $W_1, W_2, \cdots, W_t$ are unramified in H (Lemma 13, Section 2) and K_1/V is tamely ramified (Lemma 12, Section 2), and hence K_1/V is unramified (Lemma 17, Section 2). Therefore assumption (3) implies that $K_1 = K$, i.e., $H = G(K^*/K)$, which gives (C). (D) is only a rephrasing of (C). (E) follows from (D) and Lemma 28 of Section 9.

Now assume that W_j and W_k have a point P in common and let P^* be a point in $\phi^{-1}(P)$. Then $P^* \in W^*_j$ and $P^* \in W^*_k$ so that $G_i(W^*_j/W_j) \subset G_i(P^*/P)$ and $G_i(W^*_k/W_k) \subset G_i(P^*/P)$ (Lemma 10, Section 2), i.e., a_j and a_k are in $G_i(P^*/P)$. Now assumption (2) implies that P is a normal crossing of $\Delta(K^*/V)$, and hence, by Proposition 1 (Section 2), $G_i(P^*/P)$ is abelian; therefore a_j and a_k commute, which proves (F). Finally, (G) follows from (D) and (F).

12. Fundamental weak parent groups.

THEOREM 2. *Let K be an n dimensional algebraic function field over an algebraically closed ground field k, let V be a nonsingular projective model of K/k, and let W be a pure $n-1$ dimensional subvariety of V with irreducible components $W_1, W_2, \cdots, W_t$. Assume that:*

(1) $\dim |W_j| > 1$ *for* $j = 1, 2, \cdots, t$;

(2) *W has only normal crossings; and*

(3) *V is simply connected.*

Then:

(A) *$V - W$ has a tame fundamental weak parent group G generated by t generators $a_1, a_2, \cdots, a_t$ with a weak parent map f of G onto $\pi'(V-W)$ such that, in each member H of $\pi'(V-W)$, a_j (i.e., the f image of a_j) generates the cyclic (and normal in H) inertia group over W_j of the unique irreducible subvariety corresponding to W_j on a normalization of V in the galois extension of K corresponding to H; also, a_j and a_k commute in G if W_j and W_k have a point in common.*

(B) *Every unrestricted tame fundamental weak parent group*[11] *of $V-W$ is t-step nilpotent.*

(C) *If $W_1, W_2, \cdots, W_t$ are pairwise connected, then every unrestricted tame fundamental weak parent group*[11] *of $V-W$ is abelian.*

(D) $\pi^*(V-W) = \pi'(V-W)$.

Proof. First we assert that (α): *$\pi'(V-W)$ contains an ascending cofinal sequence*; we shall give several proofs of this. (i) By Theorem 1, $\pi'(V-W)$ is finitely generated, and hence (α) follows from Proposition 3 of Section 8.[12] (ii) For any K^* as in Theorem 1, $G = G(K^*/K)$ and the generators $a_1, a_2, \cdots, a_2$ satisfy the description given before Lemma 23 of Section 8; using the notation of that description, we can set $n_j(K^*) =$ order of a_j in G_j; note that $n_j(K^*)$ does not depend on the particular generator a_j of $G_i(W^*_j: W_j)$.[13] Then in view of the fact that the inertia groups project

[11] In particular, G and the inverse limit of $\pi'(V-W)$, i.e., the galois group over K of the compositum of $\Omega'_g(V-W)$, as well as every unrestricted tame fundamental parent group of $V-W$.

[12] Proposition 3 is based on the general group theoretic Lemmas 18 and 19 and also on Lemmas 20 and 21, whereas Lemma 24 is based on Lemma 23 dealing with 'nice' groups, and so the proof of Lemma 24 is less sophisticated than that of Proposition 3.

[13] G will stand for $G(K^*/K)$ only in this sentence and should not be confused with

properly (Lemma 2 of Section 2), taking compositums and applying Lemma 24 of Section 8, we conclude the following:[12] Given galois extensions K_1 and K_2 of K which are tamely ramified over V and for which $\Delta(K_1/V)$ and $\Delta(K_2/V)$ are contained in W, $n_j(K_1)=n_j(K_2)$ for $j=1,2,\cdots,t$ implies that $K_1=K_2$, and $n_j(K_1)$ divides $n_j(K_2)$ for $j=1,2,\cdots,t$ implies that $K_1\subset K_2$. From this, it follows that $\pi'(V-W)$ is countable; and hence we can conclude (α) from Lemma 20 of Section 8, or we may proceed thus: Let $m_1,m_2,\cdots$ be a sequence of positive integers such that m_q divides m_{q+1} for all q and any positive integer divides some m_q; for instance, take $m_q=q\,!$. By Lemma 24, there exists a unique (finite) galois extension K_q (in a fixed algebraic closure of K) tamely ramified over V, with $\Delta(K_q/V)\subset W$, for which $n_j(K_q)$ divides m_q for $j=1,\cdots,t$ and such that K_q contains every other finite galois extension of K with these properties. Again by Lemma 24, it follows that $G(K_1/K)<G(K_2/K)<\cdots<G(K_q/K)<G(K_{q+1}/K)<\cdots$ is a cofinal ascending sequence in $\pi'(V-W)$. (iii) Since there are only a finite number of tamely ramified coverings of V of a given degree with branch loci contained in W (Remark 9 of Section 6 of [A3]),[4] (α) follows from the trivial Lemma 21 of Section 8.

Now let $1=G^1<G^2<\cdots$ be an ascending cofinal sequence in $\pi'(V-W)$, let $K=K^1\subset K^2\subset\cdots$ be the corresponding galois extensions of K with $G(K^q/K)=G^q$, and let ϕ_q be the rational map of a K^q-normalization of V onto V. By Theorem 1, $\phi_q^{-1}(W_j)$ is irreducible; let

$$G^q{}_j=G_i(\phi_q^{-1}(W_j)/W_j).$$

Theorem 1 tells us that $G^q{}_1,G^q{}_2,\cdots,G^q{}_t$ are cyclic normal subgroups of G^q and they generate G^q. We shall show that generators $b^q{}_j$ of $G^q{}_j$ can be so chosen that for all q, we have $u_{q+1}(b^{q+1}{}_j)=b^q{}_j$ for $j=1,2,\cdots,t$, where u_{q+1} is the canonical homomorphism of G^{q+1} onto G^q. For $q=1$, we of course have $b^1{}_1=b^1{}_2=\cdots=b^1{}_t=1$; now suppose $q>1$ and that $b^h{}_j$ have been so chosen for all $h<q$. Lemma 2 of Section 2 tells us that $u_{q+1}^{-1}(G^q{}_j)=G^{q+1}{}_j$, and hence $u_{q+1}^{-1}(b^q{}_j)$ is a generator of $G^{q+1}{}_j$ and we set $b^{q+1}{}_j=u_{q+1}^{-1}(b^q{}_j)$. Since $G^1<G^2<\cdots$ is cofinal in $\pi'(V-W)$, invoking Lemma 22 of Section 8, we can find a group G on t generators $a_1,a_2,\cdots,a_t$ and a weak parent map f of G onto $\pi'(V-W)$ such that the f image of a_j in G^q is $b^q{}_j$ for all q and $j=1,\cdots,t$. Again since $G^1<G^2<\cdots$ is cofinial in $\pi'(V-W)$, it follows from Lemma 2 of Section 2, conclusion (F) of Theorem 1 and

the G in the conclusion (A) of Theorem 2. Also only in this sentence, the notation of Theorem 1 is used, for instance $W^*{}_j$, etc.

Proposition 4 of Section 9 that G satisfies the description of conclusion (A) of Theorem 2 with respect to the set of generators $a_1, a_2, \cdots, a_t$ and the weak parent map f. (B) and (C) follow from (A) and conclusions (E) and (G) of Theorem 1 by invoking Proposition 4 of Section 9. (D) is given in conclusion (B) of Theorem 1. Q. E. D.

Remark 8. Referring to the conclusion (A) of Theorem 2, Lemma 22 of Section 8 tells us that G is unique in the following sense. If G' is a group on t generators $a'_1, a'_2, \cdots, a'_t$ with a weak parent map f' of G' onto $\pi'(V - W)$ such that for $j = 1, 2, \cdots, t$, and for each H in $\pi'(V - W)$, the f and f' images respectively of a_j, a'_j coincide, i. e., a_j and a'_j are mapped onto the *same* generator of the said inertia group, then there exists a unique isomorphism of G onto G' with $a_j \to a'_j$ for $j = 1, \cdots, t$. This Remark applies to Theorem 3 of the next section as a special case.

Remark 9. In deducing Theorem 2 above and Theorem 3 of the next section from Theorem 1, one could probably pass to the compositum of $\Omega'_g(V - W)$ and use ramification theory of infinite galois extension.

Remark 11. In this remark, we shall be speaking very roughly and approximately. From the proofs of Theorems 1 and 2, it is clear that if we do not assume V to be simply connected, then the same methods would give us information about the kernel of the natural homomorphism of the fundamental group of $V - W$ onto the fundamental group of V and would imply that this kernel has approximately the description given for the fundamental group of $V - W$ in these theorems. Thus we would get the effect of removing W on the fundamental group of V. In the same vein, if W_1 and W_2 are two subvarieties of V satisfying suitable assumptions, then those methods would give a description for the kernel of the natural homomorphism of the fundamental group of $V - W_1 - W_2$ onto the fundamental group of $V - W_1$. We shall exploit these things in a later communication.

Remark 12. The assumption in Theorems 1 and 2 that $\dim |W_j| > 1$ can be replaced by the weaker assumption that $\dim |mW_j| > 1$ for some positive integer m and that there exists a prime divisor in the linear system $|mW_j|$. This remark, in conjunction with our forthcoming work on fundamental groups for branch loci with higher singularities, will be applied to deducing theorems on the nonexistence of irreducible plane curves of a given degree and prescribed singularities.

D. Applications.

13. Theorem of Zariski. As an application of Theorem 1, we shall now deduce the following results which, in the classical case (i.e. for the ground field of complex numbers), is due to Zariski.

THEOREM 3. *Let P_n be the n dimensional projective space over k with $n > 1$, let W be a hypersurface in P_n with normal crossings only, let $g^*_1, g^*_2, \cdots, g^*_t$ be the orders of the irreducible components of W. Let $d = 1$ in case $p = 0$ and $d =$ the highest power of p which divides $g^*_1, g^*_2, \cdots, g^*_t$ in case $p \neq 0$; let $g_j = g^*_j d^{-1}$, and let G be the abelian group on t generators $a_1, a_2, \cdots, a_t$ with the only relation*

$$a_1^{g_1} a_2^{g_2} \cdots a_t^{g_t} = 1.$$

Then G is a tame fundamental parent group of $V - W$. Also, $\pi^*(V - W) = \pi'(V - W)$, and hence G is a reduced fundamental parent group of $V - W$ as well. G is a direct product of a free abelian group on $t - 1$ generators and a cyclic group of order equal to the greatest common divisor of $g_1, g_2, \cdots, g_t$, i.e., equal to the greatest common divisor of $g^*_1, g^*_2, \cdots, g^*_t$ in case $p = 0$ and to the part of this prime to p in case $p \neq 0$.

First, we shall give three lemmas.

LEMMA 32. *Let A be a unique factorization domain with quotient field K such that A contains an alegbraically closed field k of characteristic p. Let Λ be an algebraic closure of K. Let $d_1, d_2, \cdots, d_t$ be pairwise coprime irreducible nonunits in A. Let Z be the set of all positive integers in case $p = 0$ and let Z be the set of all positive integers prime to p in case $p \neq 0$. Then we can choose elements $u_m, d_1^{1/m}, d_2^{1/m}, \cdots, d_t^{1/m}$ in Λ such that u_m is a primitive m-th root of 1 and $d_1^{1/m}, d_2^{1/m}, \cdots, d_t^{1/m}$ are m-th roots respectively of $d_1, d_2, \cdots, d_t$ such that if m and m^* are in Z with $m^* \equiv 0 \pmod m$, then $(u_{m^*})^{m^*/m} = u_m$ and $(d_j^{1/m^*})^{m^*/m} = d_j^{1/m}$ for $j = 1, 2, \cdots, t$. For m in Z, let $L_m = K(d_1^{1/m}, d_2^{1/m}, \cdots, d_t^{1/m})$. Then τ_{mj}: $d_j^{1/m} \to u_m d_j^{1/m}$, $d_q^{1/m} \to d_q^{1/m}$ for $q \neq j$ is an automorphism of L_m/K of order m; $G(L_m/K)$ is the direct product of the t cyclic subgroups of order m generated by $\tau_{m1}, \tau_{m2}, \cdots, \tau_{mt}$ respectively, so that $G(L_m/K)$ is an abelian group of order m^t. Let Ω_1 denote the set of all field extension of K contained in L_m for the various m in Z. Then Ω_1 is closed with respect to subfields and finite compositums. Hence the galois groups over K of all the various members of Ω_1 form a group tower π_1. Let F_t be the free abelian group on t generators $\alpha_1, \alpha_2, \cdots, \alpha_t$. Then there exists a unique weak parent map f of F_t onto π_1 such that if for*

M in Ω_1, we denote by $f(M)$ the homomorphism, belonging to f, of F_t onto $G(M/K)$, then we have $f(L_m)(\alpha_j) = \tau_{mj}$ for $j = 1, 2, \cdots, t$ and for all m in Z. Furthermore, if $p = 0$, then f is a parent map and if $p \neq 0$, then f is a modulo p parent map and gives an isomorphism of the modulo p derived group tower of F_t onto π_1.

Proof. The existence of u_m, $d_j^{1/m}$ follows thus: Fix an ascending sequence $1 = m_1 < m_2 < m_3 < \cdots$ of integers in Z such that m_q divides m_{q+1} for all q and each integer in Z divides some m_q. By induction on q, we shall define for $h = 1, 2, \cdots, q$, a primitive m_h-th root u_{m_h} of 1 in Λ and an m_h-th root d_j^{1/m_h} of d_j in Λ such that for all integers g, h with $1 \leqq g \leqq h \leqq q$, we have $(u_{m_h})^{m_h/m_g} = u_{m_g}$ and $(d_j^{1/m_h})^{m_h/m_g} = d_j^{1/m_g}$. For $g = 1$, we set $u_{m_1} = 1$ and $d_j^{1/m_1} = d_j$; now suppose $q > 1$ and assume that this has been done for $q - 1$. Then there exists a primitive m_q-th root v of 1 in Λ and a m_q-th root of d_j in Λ such that $(v)^{m_q/m_{q-1}} = u_{m_{q-1}}$ and $(e_j)^{m_q/m_{q-1}} = d_j^{1/m_{q-1}}$, and we can take v for u_{m_q} and e_j for d_j^{1/m_q}. Now for m in Z dividing a particular m_q, set $u_m = (u_{m_q})^{m_q/m}$ and $d_j^{1/m} = (d_j^{1/m_q})^{m_q/m}$, and observe that this is independent of m_q.

Since d_j is irreducible in A, $K(d_j^{1/m})/K$ is a galois extension with galois group cyclic of order m and generated by $d_j^{1/m} \to u_m d_j^{1/m}$. L_m is the compositum of $K(d_1^{1/m}), \cdots, K(d_t^{1/m})$; hence L_m/K is galois and $G(L_m/K)$ is naturally isomorphic to a subgroup of the direct product of $G(K(d_1^{1/m})/K)$, $\cdots, G(K(d_t^{1/m})/K)$, and hence if we showed that

$$[L_m : K] = m^t = [K(d_1^{1/m}) : K] \cdots [K(d_t^{1/m}) : K],$$

then the assertion about $G(L_m/K)$ would follow. Let v be the valuation of K given by the irreducible element d_1 of the unique factorization domain A with $v(d_1) = 1$ and let v^* be an extension of v to L_m; then $v^*(d_1^{1/m}) = 1/m$, and hence $r(v^* : v) \equiv 0 \pmod{m}$. For $j \neq 1$, d_j and d_1 are coprimes irreducibles, and hence the discriminant of $X^m - d_j$ is of v-value zero so that v is unramified in $K(d_j^{1/m})$. Hence v is unramified in $K(d_2^{1/m}, \cdots, d_t^{1/m})$ which implies that $r(v^* : K(d_2^{1/m}, \cdots, d_t^{1/m})) = r(v^* : v) \geqq m$. Now making induction on m, we can conclude that $[L_m : K] = m^t$.

It is clear that the automorphism τ_{mj} form a consistent family of generators for the cofinal set $\{G(L_m/K), m \in Z\}$ of π_1, and hence, by Lemma 22 of Section 8, we can find a (unique) group G on t generators $a_1, a_2, \cdots, a_t$ with a weak parent map $g = \{g(M) : G \to G(M/K), M \in \Omega_1\}$ such that $g(L_m)(a_j) = \tau_{mj}$ for $j = 1, 2, \cdots, t$ and $m \in Z$. By Proposition 4 of Section 9, G is abelian. Let $n_1, n_2, \cdots, n_t$ be arbitrary integers not all zero and let

$b = a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t}$. Say $n_1 \neq 0$. Then there exists m in Z with $n_1 \not\equiv 0 \pmod{m}$; let $M = K(d_1^{1/m})$. Since $g(M)$ equals $g(L_m)$ followed by the canonical homomorphism of $G(L_m/K)$ onto $G(M/K)$, we can conclude that $g(M)(a_j) = 1$ for $j = 2, 3, \cdots, t$ and $g(M)(a_1)$ is the automorphism $d_1^{1/m} \to u_m d_1^{1/m}$ and hence is of order m; therefore $g(M)(b) = (a_1^{n_1}) \neq 1$ since $n_1 \not\equiv 0 \pmod{m}$. This shows that G is the free abelian group on $a_1, a_2, \cdots, a_t$ and we can take $G = F_t$, $\alpha_j = a_j$ and $f = g$; the uniqueness follows from Lemma 22 of Section 8.

Now assume that $p \neq 0$. Since every member of Ω_1 is contained in some L_m, it follows that the order of each group in π_1 is prime to p. Observe that in $G(L_m/K)$, $m =$ order of $\tau_{mj} =$ order of τ_{mj} in the quotient group of $G(L_m/K)$ by the subgroup generated by $\tau_{m1}, \tau_{m2}, \cdots, \tau_{mj-1}$; hence Lemma 24 of Section 8 tells us that any normal subgroup of G of finite index prime to p contains $g(L_m)^{-1}(1)$ for some m in Z and hence g is a modulo p quasi parent map of G onto π_1. Now let $n_1, n_2, \cdots, n_t$ be arbitrary integers not all zero and let $b = a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t}$. Say $n_1 \neq 0$. Then there exists m in Z with $n_1 \not\equiv 0 \pmod{m}$. Let $L = K(d_1^{1/m})$. Then $g(L)(b) = g(L)(a_1)^{n_1} \neq 1$ since the order of $g(L)(a_1)$ is m. Therefore g is a modulo p parent map. If $p = 0$, omitting any reference to p in the above argument, we conclude that g is a parent map.

LEMMA 33. *Let the situation be as Lemma 32. Let $g^*_1, g^*_2, \cdots, g^*_t$ be given positive integers. Let $d = 1$ in case $p = 0$ and let $d =$ the highest power of p which divides $g^*_1, g^*_2, \cdots, g^*_t$ in case $p \neq 0$. Let $g_j = g^*_j d^{-1}$. Let N be the subgroup of F_t generated by*

$$\beta = \alpha_1^{g_1}\alpha_2^{g_2}\cdots\alpha_t^{g_t}.$$

Let q be the canonical homomorphism of F_t onto $G = F_t/N$ and let $a_j = q(\alpha_j)$. Let π' be a subtower of π_1 and let Ω' be the corresponding subset of Ω_1. Assume that $L \in \Omega_1$ and $G(L/K)$ cyclic implies that $L \in \Omega'$ if and only if

$$f(L)(\alpha_1)^{g^*_1} f(L)(\alpha_2)^{g^*_2}\cdots f(L)(\alpha_t)^{g^*_t} = 1. \tag{I}$$

Then

$$N = \bigcap_{L \in \Omega'} f(L)^{-1}(1),$$

so that for each L in Ω', there exists a unique homomorphism $\phi(L)$ of G onto $G(L/K)$ with $f(L) = \phi(L)q$, and $\phi = \{\phi(L), L \in \Omega'\}$ is a weak parent map of G onto π'. Furthermore, if $p = 0$ then ϕ is a parent map, and if $p \neq$ then ϕ is a modulo p parent map. G is a direct product of a free abelian group on $t - 1$ generators and a cyclic group whose order is the greatest common divisor of $g_1, g_2, \cdots, g_t$.

Proof. Let E be a finitely generated abelian group; then E is a direct sum of cyclic subgroups $E_1, E_2, \cdots, E_n$; let e_h be the projection of E onto E_h, then given $x \in E$ with $x \neq 1$, there exists h such that $e_h(x) \neq 1$. Using this argument, we can at once conclude that given *any* $L \in \Omega_1$, $L \in \Omega'$ if and only if (I) holds. Let N^* be the cyclic subgroup of F_t generated by

$$\beta^* = \alpha_1^{g^*_1}\alpha_2^{g^*_2} \cdot \cdot \cdot , \alpha_t^{g^*_t}.$$

Then for all L in Ω', $N^* \subset f(L)^{-1}(1)$ so that there exists a unique homomorphism $\phi^*(L)$ of $G^* = F_t/N^*$ onto $G(L/K)$ such that $f(L)$ equals the canonical homomorphism of F_t onto G^* followed by $\phi^*(L)$. If $p = 0$, then f is a parent map and hence, invoking Lemma 27 of Section 9, we conclude that $\phi^* = \phi$ is a parent map of $G^* = G$. Now assume that $p \neq 0$. Since f is a modulo p parent map of F_t onto π_1, we conclude that $\phi^* = \{\phi^*(L), L \in \Omega'\}$ is a modulo p quasi parent map of G^* onto π'. Let x be the greatest common divisor of $g^*_1, g^*_2, \cdots, g^*_t$, let p^y be the highest power of p which divides x and let $z = xp^{-y}$. Let $h_j = g^*_j x^{-1}$ and let

$$\gamma = \alpha_1^{h_1}\alpha_2^{h_2} \cdot \cdot \cdot \alpha_t^{h_t},$$

so that $\beta = \gamma^z$ and $\beta^* = \gamma^x$. Since the greatest common divisor of $h_1, h_2, \cdots, h_t$ is 1, by well known properties of finitely generated free abelian groups, we can find $\gamma_2, \gamma_3, \cdots, \gamma_t$ such that $\gamma = \gamma_1, \gamma_2, \cdots, \gamma_t$ is a free abelian basis of F_t. Let $k = k_1, k_2, \cdots, k_t$ be the images in G^* of $\gamma_1, \gamma_2, \cdots, \gamma_t$ respectively. Then G^* is a direct sum of the free abelian group V_2 generated by the free generates $k_2, k_3, \cdots, k_t$ and the cyclic group V_1 generated by k_1. Let v_j be the projection of G^* onto V_j. For all L in Ω', the order of $\phi^*(L)(k_1)$ is prime to p, and hence it divides z so that $\phi^*(L)(k_1^z) = 1$. Now let $u_1, u_2, \cdots, u_t$ be arbitrary positive integers and let $h = k_1^{u_1}k_2^{u_2} \cdot \cdot \cdot k_t^{u_t}$. Assume that $\phi^*(L)(h) = 1$ for all L in Ω'. Applying the consideration of the last paragraph in the proof of Lemma 32 to V_2, we conclude, via v_2, that $u_2 = u_3 = \cdot \cdot \cdot = u_t = 0$. Next, let τ be a homomorphism of the cyclic group V_1 of order x onto a cyclic group of order z. Then τv_1 maps V onto a finite group of order prime to p, and hence there exists L in Ω' such that the kernels of τv_1 and $\phi^*(L)$ coincide. Therefore $\phi^*(L)(k_1)$ is of order z. Since $\phi_0(L)(k_1^{u_1}) = \phi^*(L)(h) = 1$, we conclude that $u_1 \equiv 0 \pmod z$. This shows that $\bigcap_{L \in \Omega'} \phi^*(L)^{-1}(1)$ is generated by k_1^z. Therefore ϕ is a modulo p parent map of G onto π'.

The following lemma is well known; we give it here for the sake of completeness.

LEMMA 34. *The projective n dimensional space P_n over k is simply connected.*

Proof. We shall make induction on n. For $n = 1$, this is well known (Proposition 3 of Section 3 of [A3]); now assume that $n > 1$ and that P_{n-1} is simply connected. Let K^* be a finite separable algebraic extension of $k(P_n)$ which is unramified over P_n let, $[K^*: k(P_n)] = m$, let V^* be a K^*-normalization of P_n and let ϕ be the rational map of V^* onto P_n. Since the hyperplanes of P_n form a linear system of dimension greater than one and is without fixed components, by the generalized Bertini theorem (Section 4), we can find a hyperplane P_{n-1} in P_n such that $U^* = \phi^{-1}(P_n)$ is irreducible, and since $Q(P_{n-1}, P_n)$ is unramified in K^*, we must have $[(U^*): k(P_{n-1})] = [K^*: k(P_n)] = m$ (Section 2). Since k is algebraically closed and K^*/P_n is unramified, for each point of P_n, there are exactly m points on V^*, and hence, for each point of P_{n-1}, there are exactly m points on U^*, and hence $k(U^*)/P_{n-1}$ is unramified. Therefore, by the induction hypothesis, $k(U^*) = k(P_{n-1})$, i.e., $m = 1$, i.e., $K^* = k(P_n)$.

Proof of Theorem 3. Since $n > 1$, the dimension of the complete linear system determined by an hypersurface in P_n is greater than 1 and any two hypersurfaces in P_n have a point in common; also, by Lemma 34, P_n is simply connected. Therefore, by Theorem 1, each group in $\pi'(P_n - W)$ is abelian and also $\pi^*(P_n - W) = \pi'(P_n - W)$. Now fix an algebraic closure Λ of $K = k(P_n)$. Choose an affine coordinate system $x_1, x_2, \cdots, x_n$ in P_n such that the hyperplane at infinity is not in W. Then $K = k(x_1, x_2, \cdots, x_n)$ and W_j is given by an irreducible polynomial $d_j = d_j(x_1, x_2, \cdots, x_n)$ of degree g^*_j in the polynomial ring $A = k[x_1, x_2, \cdots, x_n]$. Now A is unique factorization domain and $d_1, d_2, \cdots, d_t$ are pairwise coprime irreducible nonunits in A. Hence we can apply Lemma 33; we shall use the notation of that lemma. We shall show that $\Omega'_g(P_n - W) \subset \Omega_1$. Since each member of $\Omega'_g(P_n - W)$ is an abelian extension of K and since an abelian extension is a compositum of cyclic extensions, it is enough to show that each cyclic extension of K contained in $\Omega'_g(P_n - W)$ is contained in Ω_1. So let L be in $\Omega'_g(P_n - W)$ such that L/K is cyclic. Let $[L: K] = m$. Since $\pi'(P_n - W) = \pi^*(P_n - W)$, m is prime to p in case $p \neq 0$, and hence there exists a polynomial

$$X^m - y \tag{1}$$

with y in K such that L is the root field of K in Λ. We can arrange matters so that $y \in A$ and that y is not divisible by the m-th power of any nonunit in A. Then the hyperplanes in P_n given by irreducible factors of y must be

ramified in L, and hence, after multiplying y by a suitable element of k, we have:

$$y = d_1^{v_1} d_2^{v_2} \cdots d_t^{v_t}. \tag{2}$$

Hence $L \subset L_m$, i.e., $L \in \Omega_1$. Thus $\Omega'_g(P_n - W) \subset \Omega_1$.

Next, let L be any member of Ω_1 such that $G(L/K)$ is cyclic. *We assert that* $L \in \Omega'_g(P_n - W)$ *if and only if*

$$f(L)(\alpha_1)^{g^*_1} f(L)(\alpha_2)^{g^*_2} \cdots f(L)(\alpha_t)^{g^*_t} = 1. \tag{3}$$

Let $[L: K] = m$ and arrange matters so that L is a rootfield of (1), where y is given by (2). Then the part of $\Delta(L/P_n)$ at finite distance is contained in W, and hence $\Delta(L/P_n) \subset W$ if and only if the hyperplane at infinity is not ramified in L. It is easily verified that the hyperplane at infinity is not ramified in L if and only if

$$v_1 g^*_1 + v_2 g^*_2 + \cdots + v_t g^*_t \equiv 0 \pmod{m}. \tag{4}$$

Note that $L \subset L_m$ and that $f(L_m)(\alpha_j) = \tau_{mj}$; let e be the canonical homomorphism of $G(L_m/K)$ onto $G(L/K)$. Then $f(L) = ef(L_m)$, and hence (3) is equivalent to

$$\prod_{h=1}^{t} e(\tau_{mh})^{g^*_h} = 1, \tag{3'}$$

i.e., to

$$e[\prod_{h=1}^{t} \tau_{mh}{}^{g^*_t}] = 1, \tag{3*}$$

i.e., to

$$\tau = \prod_{h=1}^{t} \tau_{mh}{}^{g^*_h} \in e^{-1}(1) = G(L_m/L) \subset G(L_m/K). \tag{5}$$

Thus we have to show that (4) is equivalent to (5). Next,

$$d = \prod_{h=1}^{t} (d_h{}^{1/n})^{v_h}$$

is a primitive element of L/K, and hence the automorphism τ of L_m/K is in $G(L_m/L)$ if and only if $\tau(d) = d$. Now

$$\begin{aligned}
\tau(d) &= \prod_{j=1}^{t} \tau_{mj}{}^{g^*_j} [\prod_{h=1}^{t} (d_h{}^{1/m})^{v_j}] \\
&= \prod_{j=1}^{t} [\tau_{mj}{}^{g^*_j} (\prod_{h=1}^{t} (d_h{}^{1/m})]^{v_j} \\
&= \prod_{j=1}^{t} [u_m{}^{g^*_j} (d_j{}^{1/m})]^{v_j} \\
&= \prod_{j=1}^{t} [u_m{}^{v_j g^*_j} (d_j{}^{1/m})^{v_j}] \\
&= [(u_m)^{v_1 g^*_1 + v_2 g^*_2 + \cdots + v_t g^*_t}] d.
\end{aligned}$$

Hence $\tau(d) = d$ if and only if

$$(u_m)^{v_1 g^*_1 + v_2 g^*_2 + \cdots + v_t g^*_t} = 1,$$

i.e., if and only if (4) holds. This proves the italicized assertion. Now the theorem follows from Lemma 33.

Remark 13. Referring to Theorem 3, let G^* be the abelian group generated by t generators $a^*_1, a^*_2, \cdots, a^*_t$ and the only relation

$$a^*_1{}^{g^*_1} a^*_2{}^{g^*_2} \cdots a^*_t{}^{g^*_t} = 1.$$

Then it follows from the proof of Lemma 33 that for $p = 0$, $G^* = G$, i.e., G^* is a (tame, reduced) fundamental parent group of $P_n - W$; and for $p \neq 0$, G^* is a modulo p quasi parent group of $\pi'(P_n - W) = \pi^*(P_n - W)$.

14. Theorem of Picard. As another application of our main results, we shall deduce a result (Theorem 5 below) which, for dimension two in the classical case, was asserted by Picard. In the following Definition, and in Lemmas 35, 36 and Theorem 4, K is an n dimensional algebraic function field over k, Λ is a fixed algebraic closure of K and V is a normal projective model of K/k.

Definition. Let W be an irreducible $n - 1$ dimensional subvariety of V. Since linear equivalence preserves degress (in the embedding projective space of V), it follows that the positive integers m such that there exists a divisor D on V with $W \equiv mD$ are bounded, the maximum of these integers will be called *the embedding degree of W in V and will be denoted by* $\delta(W, V)$. Also, we define *the reduced embedding degree* $\delta(W, V)$ *of W in V* by setting it equal to $\delta^*(W, V)$ in case $p = 0$ and equal to $\delta^*(W, V)$ divided by the highest power of p which divides $\delta^*(W, V)$ in case $p \neq 0$. It is obvious from the definition that $\delta^*(W, V)$ and hence $\delta(W, V)$ is a biregular invariant. The biregular invariance of $\delta(W, V)$ will also follow from Lemma 36 and from that lemma, it will also follow that $\delta(W, V)$ equals the maximum as well as the least common multiple of all integers m prime to p (respectively, all integers m) in case $p \neq 0$ (respectively, $p = 0$) for which there exists a divisor D on V with $W \equiv mD$. Also note that if V is a projective space P_n, then $\delta^*(W, V)$ is the usual order of the hypersurface of W; and in this case, $\delta(W, V)$ will also be called *the reduced order of W*.

LEMMA 35. *Let V^* be a normalization of V in a finite separable algebraic extension K^* of K and assume that V^* is simply connected. Then*

any one of the following two conditions implies that V is simply connected: (1) there exist an irrreducible subvariety of V^* whose ramification index over K equals $[K^*: K]$; (2) any field between K and K^* other than K is ramified over V.

Proof. In view of Lemma 4 of Section 2 of [A2], (1) implies (2). Now assume (2). Let K_1 be any finite separable algebraic extension of K such that K_1/V is unramified. Let K^*_1 be a compositum of K^* and K_1. Then by Lemma 9 of Section 2, K^*_1/V^* is unramified. Hence $K^*_1 = K^*$, i. e., $K_1 \subset K^*$ which, in view of (2), implies that $K_1 = K$.

LEMMA 36. *Let W be an irreducible $n-1$ dimensional subvariety of V. Assume that V is nonsingular and simply connected. Let K^* be the compositum of all finite abelian extensions of K which are tamely ramified over V and for which the branch locus over V is contained in W. Then K^*/K is a cyclic extension of degree $\delta(W, V)$.*

Proof. Let L/K be a finite abelian extension in Λ such that L/V is tamely ramified and $\Delta(L/V) \subset W$; let V^* be a L-normalization of V and let ϕ be the rational map of V^* onto V. Since L/K is abelian and since the inertia groups over K of the various irreducible components of $\phi^{-1}(W)$ are K-conjugates, all these inertia groups must be the same; let L^* be the fixed field of this inertia group. There L/L^* is cyclic (Lemma 14, Section 2), and L^*/V is unramified (Lemmas 13 and 17, Section 2); since V is simply connected, we have $L^* = K$; *this also shows that $[L: K]$ = ramification index over K of any irreducible component of $\phi^{-1}(W)$.*

Therefore it is enough to show that for an integer $m > 1$, which is prime to p in case $p \neq 0$, there exists a cyclic extension L/K of degree m such that L/V is tamely ramified and $\Delta(L/V) \subset W$ if and only if there exists a divisor D and V with $W \equiv mD$. Assume that L exists; then L/K is the root field of a polynomial $X^m - y$ with $y \in K$. Then $\Delta(L/V)$ contains each of the prime divisors which occur in the divisor (y) of the function y with a coefficient which is not divisible by m. By the above italicized remark, it follows that W occurs in (y) with a coefficient q which is prime to m. Then we can find an integer q^* prime to m such that $qq^* \equiv 1 \pmod{m}$. Replacing y by y^q, we can assume that $q \equiv 1 \pmod{m}$, which implies that $(y) - W$ is equal to m times a divisor D so that $W \equiv mD$. Conversely, assume that D exists. Then there exists y in K such that $(y) = W - mD$, and we may take L to be the root field over K of the polynomial $X^m - y$.

THEOREM 4. *Let W be an irreducible subvariety of V. Assume that W*

has only normal crossings and $\dim |W| > 1$ *and that* V *is simply connected. Let* K^* *be the compositum of all the fields in* $\Omega'_g(V-W)$. *Then* (i) K^*/K *is cyclic of degree* $\delta(W, V)$; *and* $V-W$ *has as a tame (as well as reduced) fundamental parent group a cyclic group of order* $\delta(W, V)$. *Let* V^* *be a* K^**-normalization of* V *and let* ϕ *be the map of* V^* *onto* V *(so that* $V^*-\phi^{-1}(W)$ *is the "tame universal covering" of* $V-W$). *Then* (ii) $V^*-\phi^{-1}(W)$ *is tamely simply connected. Finally,* (iii) *the normalization of* V *in any field between* K *and* K^* *(in particular,* V^**) is simply connected.*

Proof. That each group in $\pi'(V-W)$ is abelian is exactly Theorem 1 for $t=1$. However, the argument for $t=1$ is rather easier and is briefly thus: For K_1 in $\Omega'_g(V-W)$, let V_1 be a K_1-normalization of V and let ϕ_1 be the rational map of V_1 onto V. Then by Proposition 6 of Section 11, $W_1 = \phi_1^{-1}(W)$ is irreducible, and hence K is itself the splitting field of W_1/W. Then K_1/K_2 is cyclic (Lemma 14, Section 2) and K_2/V is unramified (Lemmas 13 and 17, Section 2); since V is simply connected, we have $K_2 = K$. Now (i) follows from Lemma 36 above. (ii) follows from (i) in view of Lemma 9 of Section 2. From (i), it follows that V^* is simply connected (Lemma 29 of Section 10) and this, together with Lemma 35 above and the italicized statement in the proof of Lemma 36, gives (iii).

PROPOSITION 7. *Let* V^* *be a normal projective variety over* k. *Assume that there exists a rational map* ϕ *of* V^* *onto a nonsingular projective simply connected variety* V *of finite index such that:* (1) ϕ *and* ϕ^{-1} *are both free from fundamental points,* (2) V^*/V *is tamely ramified,* (3) $\Delta(V^*/V)$ *is irreducible,* (4) $\Delta(V^*/V)$ *has only normal crossings, and* (5) $\dim |\Delta(V^*/V)| > 1$. *Then* V^* *is simply connected,* $k(V^*)/k(V)$ *is galois with galois group cyclic of order dividing* $\delta(\Delta(V^*/V), V)$, *and* $V^*-\phi^{-1}(\Delta(V^*/V))$ *is tamely simply connected in case* $[k(V^*) : k(V)] = \delta(\Delta(V^*/V), V)$.

Proof. This is essentially Theorem 4 stated from a covering to the projection instead of the other way around.

PROPOSITION 8. *Let* W *be an irreducible hypersurface of reduced degree* g *with normal crossings only in projective* n *dimensional space* P_n *over* k. *Let* K^* *be the compositum of all the fields in* $\Omega'_g(P_n-W)$. *Then* (i) $K^*/k(P_n)$ *is cyclic of degree* g *so that* P_n-W *has for a tame (as well as reduced) fundamental parent group a cyclic group of order* g. *Let* V^* *be a* K^**-normalization of* P_n *and let* ϕ *be the rational map of* V^* *onto* P_n. *Then* (ii) $V^*-\phi^{-1}(W)$ *is tamely simply connected. Finally,* (iii) *the normaliza-*

tion of P_n in any field between $k(P_n)$ and K^* (in particular, V^*) is simply connected.

Proof. For $n=1$, this means that $P_1 - W$ (W is a point) is tamely simply connected and P_1 is simply connected; this is well known (Proposition 6 of Section 3 of [A3]); now assume that $n>1$. Then this proposition follows from Theorem 4 in view of Lemma 34 of Section 13 or, alternatively, (i) is exactly Theorem 3 for $t=1$ and (i) and (iii) follow from (i) as in the proof of Theorem 4.

THEOREM 5. *Let V^* be a hypersurface in projective $n+1$ dimensional space P_{n+1} having an affine equation*

$$X_{n+1}{}^{m} - f(X_1, X_2, \cdots, X_n) = 0,$$

where $W: f(X_1, X_2, \cdots, X_n) = 0$ is an irreducible hypersurface (i. e., f is an irreducible polynomial) in projective n space P_n (with affine coordinates $X_1, X_2, \cdots, X_n$) having only normal crossings (in particular, say, W is to be nonsignular, or 'generic'), such that m divides the reduced order g of W. Then V^* is simply connected. If $m=g$, then $V^* - (f(X_1, X_2, \cdots, X_n) = 0 \cap V^*)$ is tamely simply connected.

Proof. Project V^* on P_n by the natural projection and call this projection map ϕ. By the Jacobian criterion, the singularities of V^* lie above the singularities of W, and hence the singular locus of X^* is of dimension less than $n-1$. Therefore V^* is normal. That ϕ and ϕ^{-1} are free from fundamental points is obvious. Now either apply Proposition 8 or apply Proposition 7 together with Lemma 34 of Section 13.

E. Classical Case and Motivation.

In this chapter, C will denote the field of complex numbers, no reference will be made to the Zariski topology, V will denote a normal projective model of an n dimensional algebraic function field over an algebraically closed ground field k of characteristic p and W will denote a proper subvariety of V. Also, π_1 will denote the usual topological fundamental group of a topological space, and furthermore, $\Gamma\pi_1$ will denote the intersection of all subgroups of π_1 of finite index and $\gamma\pi_1$ will denote the factor group $\pi_2/\Gamma\pi_1$. In this chapter, since its main purpose is motivation and description, we shall not try to be completely precise.

15. Existence of algebraic coverings. Suppose $k=C$, so that V becomes a topological space in the classical manner. Then $V-W$ is connected, and finite regular unramified topological coverings of $V-W$ are in one to one natural correspondence with finite homomorphic images of $\pi_1(V-W)$. Let V' be a finite unramified topological covering of $V-W$. Then by the recent work of Grauert and Remmert ([GR], see also Enriques' work on this topic in [E] and Chapter VIII of [Z2])—which can be called the general Riemann Existence Theorem—implies that V' can be uniquely completed to a normal algebraic variety V^*, thus making V^* an algebraic covering of V with $\Delta(V^*/V) \subset W$. Now if the covering V' is regular, then $k(V^*)/k(V)$ is galois and the covering group of V' over V is naturally isomorphic to the galois group $G(k(V^*)/k(V))$, and hence we can conclude that $\gamma\pi_1(V-W)$ is, in a natural way, a parent group of $\pi(V-W) = \pi'(V-W) = \pi^*(V-W)$. This explains our terms, . . . fundamental group tower . . ., in abstract algebraic geometry. Even if the Existence Theorem were not available, these group towers would, in the abstract case carry the same weight; however, in the presence of the Existence Theorem, these concepts do carry more weight for considerations of the classical case, and, for instance, from Theorem 2 (Section 12), we can at once conclude the following new result for the classical case.

PROPOSITION 9. *Suppose $k=C$. Assume that V is nonsingular, W is pure $n-1$ dimensional with irreducible components $W_1, W_2, \cdots, W_t$, and that:* (1) $\dim |W_j| > 1$ *for* $j=1,2,\cdots,t$; (2) *W has only normal crossings*; *and* (3) *V has no finite unramified topological coverings (this would certainly be so if V is topologically simply connected, i.e., if $\pi_1(V)=1$). Then $\gamma\pi_1(V-W)$ is t-step nilpotent and it is abelian in case $W_1, W_2, \cdots, W_t$ are pairwise connected (here topological connectedness and algebrogeometric connectedness are the same). Also $V-W$ has an unrestricted tame fundamental parent group, namely $\gamma\pi_1(V-W)$.*

Now consider Theorem 3 of Section 13. In the classical case, this was proved by Zariski, namely in [Z1], also Chapter VIII of [Z2]; he proved the following:

(A) *Let W be a curve with only normal crossings in the complex projective plane P_2 and let $g_1, g_2, \cdots, g_t$ be the orders of the irreducible components of W. Then $\pi_1(P_2-W)$ is an abelian group with t generators $a_1, a_2, \cdots, a_t$ and the only relation*

$$a_1^{g_1}a_2^{g_2}\cdots a_t^{g_t}=1.$$

Then in [Z3], he proved the following theorem.

(B) *Let W be a hypersurface in complex projective n space P_n and let P_{n-1} be a generic hypersurface in P_n. Then*

$$\pi_1(P_n - W) \text{ and } \pi_1(P_{n-1} - P_{n-1} \cap W)$$

are naturally isomorphic.

Putting together (A) and (B), invoking the Existence Theorem of Grauert-Remmert, and observing that in a finitely generated abelian group, the intersection of subgroups of finite index is 1 (Lemma 27 of Section 9), there results Theorem 3 in case $k = C$. Also note that Theorem 3 gives an evidence of (B) in the abstract case.

Next, consider Theorem 5 of Section 14. For $n = 2$ and $k = C$, this was asserted by Picard (Sections 12-14 of Chapter IV of [PS]) in connection with his statement that any nonsingular surface in complex projective three space is simply connected. Note that in the classical case, in view of (B) above, the theorem for general n follows from the case $n = 2$.

16. Finite generation of fundamental groups. Consider the following statement which one expects to be true: (α) *Let W be a subvariety of an algebraic variety V over C; then V can be triangulated so as to make W a subcomplex.* Now (α) implies that $\pi_1(V - W)$ is finitely generated; for instance, take the third barycentric subdivision of V, then $V - W$ can be 'projected' onto a (closed) subcomplex X of $V - W$, thus making X a deformation retract of $V - W$; hence $\pi_1(V - W) = \pi_1(X)$ and, X being a finite complex, $\pi_1(X)$ is the fundamental group of a 'tree' and hence is finitely generated. Hence the group tower $\pi(V - W) = \pi'(V - W) = \pi^*(V - W)$ has a finitely generated parent group and, in particular, a finitely generated weak parent group. This is the reason why we have included *finite generation* in the definitions of (1) a tame fundamental parent group, (2) a reduced fundamental parent group, (1*) a tame fundamental weak parent group, and (2*) a reduced fundamental weak parent group. The reason for not at all defining, in case of $p \neq 0$, a fundamental parent (respectively: weak parent) group, say as a finitely generated unrestricted fundamental parent (respectively: weak parent) group, is that the entire group tower (including tame as well as untame coverings) can be way too large(as is exhibited in [A3, 4], and in general we do not expect it to have a finitely generated parent or weak parent group.

The explanation of the concepts (1*) and (2*) is now complete. However, concerning the concepts of (1) a tame fundamental parent group G of $V-W$ and (2) a reduced fundamental parent group G^* of $V-W$, we must explain one point, namely that in case of nonzero characteristic $p \neq 0$, G (respectively: G^*) is required to be just a little less than a finitely generated parent group of $\pi'(V-W)$ (respectively: $\pi^*(V-W)$), namely we have required that G (respectively: G^*) be finitely generated and that there exist a weak parent map f of G (respectively: G^*) onto $\pi'(V-W)$ (respectively: $\pi^*(V-W)$) such that the kernel of f include all the normal subgroups of G (respectively: G^*) of finite index *prime to* p. The reason for this is that in general there does not exist a finitely generated parent group of $\pi'(V-W)$ (respectively: $\pi^*(V-W)$); for instance, certainly we can have a situation in which $\pi'(V-W)$ and $\pi^*(V-W)$ are isomorphic to the modulo p derived group tower of an infinite cyclic group—for instance, take V to be the projective line and for W, take two points (Proposition 6 of Section 3 of [A3]), or take V to be the projective plane and for W, take two lines (Theorem 3 of Section 13)—and this group does not have any finitely generated parent group (Example 2 of Section 7).

Thus the complete analogue for the abstract case of the existence in the classical case of a topological fundamental group which one expects to be always finitely generated is the following statement which we state as a conjecture.

CONJECTURE 1. *For any normal projective algebraic variety V and a subvariety W, there exists a tame fundamental parent group of $V-W$.*

A proof of this conjecture would be a good contribution to the theory of coverings in the abstract case. Note that the existence of a tame fundamental parent group implies the existence of a reduced fundamental parent group. Now if one proves Conjecture 1, then out of the class of all tame fundamental parent groups, how far one can choose one (or more) which one would like to call *a fundamental group* of $V-W$, is another matter—for instance, can one somehow tell the *right* number of generators—, perhaps in the abelian case this is rather easy. A somewhat weaker form of Conjecture 1 is this:

CONJECTURE 2. *For any normal projective algebraic variety V and a subvariety W, there exists a tame fundamental weak parent group of $V-W$.*

Note that for $V-W$, an unrestricted tame (respectively: reduced) fundamental weak parent group exists trivially, for instance, the inverse limit

of $\pi'(V-W)$ (respectively: $\pi^*(V-W)$) will do. In general, the possible existence of an unrestricted tame (respectively: reduced) fundamental parent group does not follow from such general considerations. However, note that in the situation of Theorem 2 of Section 12, in case the W_j are pairwise connected (and hence, in particular, in the situation of Theorem 3 of Section 13), $\pi'(V-W)=\pi^*(V-W)$ has a weak parent group which is finitely generated and abelian; now it is easily shown that if a compact abelian group G has a finitely generated dense subgroup, then every subgroup of G of finite index is closed; hence the inverse limit of $\pi'(V-W)=\pi^*(V-W)$ is an unrestricted tame (as well as reduced) fundamental parent group of $V-W$.

Also recall the result given in Remark 9 of Section 6 of [A3] (see also footnote 4 of the present paper): For any normal projective variety V and a subvariety W, there exist only a finite number of tame coverings of V of a given degree with branch loci contained in W. Note that this is a trivial consequence of Conjecture 2.

Now in this paper, we have given affirmative answers to these conjectures in certain fairly general situations, namely, in the situation of Theorem 2 (Sceion 12), we have affirmed Conjecture 2, and in Remark 8 (Section 12), we have affirmed Conjecture 3 and in the situation of Theorem 3 (Section 13), we have affirmed Conjecture 1. Returning to statement (α): the 'proof' of this given by van der Waerden [V, Appendix to Chapter III] has recently been pointed out by Whitney [W, Footnote 1] to be not entirely correct (for nonsingular V and empty W, (α) is well known). Hence, at least at the present time, the following is another contribution to the classical case.

PROPOSITION 10. *In the situation of Projosition* T (*Section* 15), *the derived group tower of $\pi_1(V-W)$ has a finitely generated (by t generators) parent group, or equivalently, the inverse limit of $\gamma\pi_1(V-W)$ contains a finitely generated dense subgroup.*

17. Miscellaneous remarks.

Remark 14. It is clear that the conjectures made in Section 4 of [A3] concerning a comparison between ramification theory in nonzero characteristic p and the ramification theory in the *corresponding* zero characteristic situation can onw be refined using the concepts of this paper; for instance, Conjecture 2 of [A3] would now be refined to read: Let S_p be a situation in nonzero characteristic p and let S_0 be the corresponding situation in characteristic zero. Then:

(The subtower of the fundamental group tower of S_0 consisting of all the members whose order is prime to p)

$$= \text{(the reduced fundamental group tower of } S_p)$$
$$\subset \text{(the tame fundamental group tower of } S_p)$$
$$\subset \text{(the fundamental group tower of } S_0),$$

where inclusion stands for being a subtower.

It is obvious that the results of the present paper give some evidence in support of this refined conjecture; to give one instance, this conjecture has been verified in the situation of Theorem 3 of Section 13; see Remark 13 of Section 13.

Remark 15. Suppose $k = C$. We do not know if the intersection of subgroups of finite index of $\pi_1(V - W)$ is 1. Observe that this is not a consequence of the (almost certain) statement that these groups are finitely generated, or even finitely presented (Chapter VIII of [Z2], page 56 and Appendix G of [K2], and [H]). Note that every finitely presented group can be realized as the fundamental group of a four dimensional real manifold (Example 3 on page 180 of [ST]). However, one does not know which groups can be the fundamental groups of algebraic varieties (complete or not).

CORNELL UNIVERSITY.

REFERENCES.

[A1] S. Abhyankar, "On the ramification of algebraic functions," *American Journal of Mathematics*, vol. 77 (1955), pp. 575-592.

[A2] ———, "Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$," *Annals of Mathematics*, vol. 63 (1956), pp. 491-526.

[A3] ———, "Coverings of algebraic curves," *American Journal of Mathematics*, vol. 79 (1957), pp. 825-856.

[A4] ———, "On the ramification of algebraic functions, Part II: Unaffected equations for characteristic two," *Transactions of the American Mathematical Society*, ———.

[A5] ———, "Local fundamental groups of algebraic, algebroid and Kroneckerian varieties," to appear.

[C1] W. L. Chow, "On the principle of degeneration in algebraic geometry," *Annals of Mathematics*, vol. 66 (1957), pp. 70-79.

[C2] ———, "On the theorem of Bertini for local domains," *Proceedings of the National Academy of Science,* ————————.

[C3] ———, "The general connectedness theorem," forthcoming.

[ES] S. Eilenberg and N. Steenrod, *Foundations of Algebraic Topology,* Princeton, 1952.

[E] F. Enriques, "Sulla costruzione delle funzioni algebriche di due variabili possendenti una data curva di diramazione," *Annali di Matematica pura ed applicata,* Serie IV, vol. 1 (1924), pp. 185-193.

[GR] H. Grauert and R. Remmert, Three notes in *Comptes Rendus de L'Academie des Sciences,* Paris, vol. 245 (1957), pp. 819-822, 882-885, 918-921.

[H] G. Higman, "A finitely generated infinite simple group," *Journal of the London Mathematical Society,* vol. 26 (1951), pp. 61-64.

[K1,2] A. G. Kurosh, *The Theory of Groups,* vols. 1 and 2, New York, 1955.

[P] L. Pontrjagin, *Topological Groups,* Princeton, 1946.

[PS] E. Picard and G. Simart, *Theorie des Fonctions Algtbrique,* Tome I, Paris (1897).

[ST] H. Seifert and W. Threlfall, *Lehrbuch der Topologie,* New York, 1947.

[V] B. L. van der Waerden, *Einführung in die Algebraische Geometrie,* New York, 1945.

[W] H. Whitney, "Elementary structure of real algebraic varieties," *Annals of Mathematics,* vol. 66 (1957), pp. 545-556.

[Z1] O. Zariski, "On the problem of existence of algebraic functions of two variables possessing a given branch curve," *American Journal of Mathematics,* vol. 51 (1929), pp. 305-328.

[Z2] ———, *Algebraic Surfaces,* New York, 1948.

[Z3] ———, "A theorem on the Poincaré group of an algebraic hypersurface," *Annals of Mathematics,* vol. 38 (1937), pp. 131-141.

[Z4] ———, "Pencils on an algebraic variety and a new proof of a theorem of Bertini," *Transactions of the American Mathematical Society,* vol. 50 (1941), pp. 48-70.

[Z5] ———, *Theory and applications of homomorphic functions on algebraic varieties over arbitrary ground fields,* New York, 1951.

[Z6] ———, "Complete linear systems on normal varieties and a generalization of a lemma of Enriques-Severi," *Annals of Mathematics,* vol. 55 (1952), pp. 552-592.

RATIONAL POINTS OF ABELIAN VARIETIES OVER FUNCTION FIELDS.*

S. LANG[1] and A. NÉRON.

We intend to give here a systematic and simplified exposition of the theorem of the base for divisors [5]. Since the appearance of [5], the theory of the Picard and Albanese varieties has become available, as well as Chow's theory of algebraic systems of abelian varieties (the K/k-trace and image). Using first an elementary equivalence criterion [9], we reduce the theorem of the base on a variety (projective, non-singular in codimension 1) to a theorem concerning the group of rational points of an abelian variety defined over a function field, by means of the above mentioned theories. We then prove the finiteness statement in two steps as usual: First, the so-called weak Mordell-Weil theorem, for which we reproduce the proof given in [3], and second the infinite descent.

We also take this opportunity of reproducing simultaneously a proof of the ordinary Mordell-Weil theorem concerning the group of rational points of an abelian variety defined over a number field, to the effect that this group is finitely generated. This proof is contained in § 3, § 5, §6, and § 7.

Aside from the above mentioned equivalence criterion, which is used only in § 1, we assume only that the reader is familiar with the basic theory of abelian varieties, as it is done for instance in [2]. We do not need the full theory of distributions, and reproduce the definition of the height of a point, together with its elementary functorial properties. This is all that is needed to carry out the infinite descent. We thus make this paper independent of [5], [6], [8].

1. The theorem of the base. If G denotes a set of geometric objects, we shall denote by G_k the subset of these objects which are rational over a field k.

Let V be a projective variety, non-singular in codimension 1, and defined over an algebraically closed field k which we may take to be a

* Received May 6, 1958.

[1] Fulbright Fellow.

universal domain. The group of divisors $D(V)_k$ contains the usual subgroups of divisors which are algebraically equivalent to 0 and linearly equivalent to 0 respectively.

$$D(V)_k \supset D_a(V)_k \supset D_l(V)_k.$$

The Picard group $D_a(V)_k/D_l(V)_k$ can be given the structure of an abelian variety, the Picard variety. The theorem of the base asserts that *the factor group $D(V)_k$ modulo $D_a(V)_k$ is of finite type, i. e. finitely generated.* We are going to show here how this theorem can be reduced to a theorem concerning abelian varieties.

Let C_u be a generic curve on V over k, depending on generic linear parameters u. This means that there is a generic linear variety L_u over k such that $C_u = V \cdot L_u$. (Cf. [1], Ch. 7.) Let J be its Jacobian, defined over the field $k(u) = K$. Let $D_0(V)_k$ be the subgroup of $D(V)_k$ consisting of those divisors $X \in D(V)_k$ such that $X \cdot C_u$ is of degree 0. Then $D(V)_k/D_0(V)_k$ is infinite cyclic, and it will suffice to prove that $D_0(V)_k/D_a(V)_k$ is of finite type.

Let $\phi \colon C_u \to J$ be a canonical map of C_u into its Jacobian, defined over the algebraic closure of $k(u)$. Then

$$\mathfrak{a} \to S(\phi(\mathfrak{a}))$$

is the canonical map of $D_a(C_u) = D_0(C_u)$ into J. We have a homomorphism

$$h \colon D_0(V)_k \to J_{k(u)}$$

given by the formula

$$h(X) = S(\phi(X \cdot C_u)).$$

According to the elementary equivalence criterion, one knows that the kernel E of h, which contains $D_l(V)_k$, is of finite type modulo $D_l(V)_k$. Hence the factor group $[E + D_a(V)_k]/D_a(V)_k$ is of finite type. To prove the theorem of the base, it will therefore suffice to prove that $D_0(V)_k/[E + D_a(V)_k]$ is of finite type.

The inverse image $h^{-1}(h(D_a(V)_k)$ is precisely equal to $E + D_a(V)_k$. We have therefore an injection

$$0 \to D_0(V)_k/[E + D_a(V)_k] \to J_{k(u)}/hD_a(V)_k.$$

Now let $\psi \colon V \to A$ be a canonical map of V into its Albanese variety. For a suitable constant $b \in A$, we have a commutative diagram

$$\begin{array}{ccc} C_u & \xrightarrow{i} & V \\ \phi \downarrow & & \downarrow \psi \\ J & \xrightarrow[i_*+b]{} & A \end{array}$$

where i_* is the induced homomorphism.

Let us look at the inverse images of divisors in $D_a(A)_k$ under the composite maps $(i_* + b) \circ \phi$ and $\psi \circ$ i. The formalism $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ can be applied to the first according to Appendix 1 of [2] since J and A are non-singular. A direct verification using intersection theory (associativity and the definition of $C_u = V \cdot L_u$) shows that it can also be applied to the second. According to the definition of the Picard variety, which one knows is obtained by pull back from the Albanese variety, we see that the map

$$h: D_a(V)_k \to J_{k(u)}$$

induces the rational homomorphism ${}^t i_*$ on $\hat{A}_k = D_a(V)_k / D_l(V)_k$, if we denote as usual by the upper index t the transpose of i_* on the Picard varieties. Consequently we have an injection

$$0 \to D_0(V)_k / [E + D_a(V)_k] \to J_{k(u)} / {}^t i_* \hat{A}_k.$$

By Chow's theory of the K/k-trace (whose definition is recalled below), one knows that $(\hat{A}, {}^t i_*)$ is a $k(u)/k$-trace of $\hat{J} = J$ ([2], Ch. 8, Th. 12). Consequently, to prove the theorem of the base, it will suffice to prove the following result.

THEOREM 1. *Let K be a finitely generated regular extension of a field k. Let A be an abelian variety defined over K, and let (B, τ) be its K/k-trace. Then $A_K / \tau B_k$ is of finite type.*

For the convenience of the reader, we recall that a couple (B, τ) consisting of an abelian variety B defined over k and an injective (i.e. purely inseparable) homomorphism $\tau: B \to A$ defined over K is said to be a *K/k-trace* of A if it satisfies the following universal mapping property: For any abelian variety C defined over an extension E of k which is free from K over k, and a homomorphism $\alpha: C \to A$ defined over KE, there exists a homomorphism $\alpha': C \to B$ defined over E such that the following diagram is commutative.

$$\begin{tikzcd} C \arrow[rr, "\alpha"] \arrow[dr, "\alpha'"'] & & A \\ & B \arrow[ur, "\tau"'] & \end{tikzcd}$$

Essentially the same arguments which will be used to prove Theorem 1 will also give us

THEOREM 2. *Let K be an algebraic number field, of finite degree over the rationals. Let A be an abelian variety defined over K. Then A_K is finitely generated.*

From these two theorems we recover immediately the fact that if K is finitely generated over the prime field, then A_K is also finitely generated. It suffices to apply the two theorems to K and the algebraic closure of the prime field in K, viewed as a constant field.

2. Reduction steps. The propositions which we prove in this section will be used to reduce our main theorem (Theorem 1) to special cases which are technically easier to handle. Throughout this section, K will denote a finitely generated regular extension of a field k. By a regular extension, we shall always mean a finitely generated one.

We first show that to prove our main theorem, we may extend our function field by a finite separable extension.

PROPOSITION 1. *Let $L \supset K$ be a finite separable extension of K, also regular over k. Let A be an abelian variety defined over K. Let $(A^{K/k}, \tau_K)$ be its K/k-trace and $(A^{L/k}, \tau_L)$ its L/k-trace. Then the factor group*

$$[\tau_L(A^{L/k})_k \cap A_K]/\tau_K(A^{K/k})_k$$

is finite.

Proof. Let Γ_L be the graph of τ_L. It is defined over L. Let us take the intersection $H = \bigcap_\sigma \Gamma_L{}^\sigma$ of Γ_L and its conjugates over K, where σ ranges over the distinct isomorphisms of L over k. Then H is K-closed and is an algebraic subgroup of $A^{L/k} \times A$. Its connected component H_0 is therefore defined over K by Chow's theorem ([2], Ch. II).

$$\Gamma_L \cap [(A^{L/k})_k \times A_K] = H \cap [(A^{L/k})_k \times A_K]$$

and this group contains $H_0 \cap [(A^{L/k})_k \times A_K]$ as a subgroup of finite index, since H_0 is of finite index in H.

We have a surjective homomorphism

$$\Gamma_L \cap [(A^{L/k})_k \times A_K] \to \tau_L(A^{L/k})_k \cap A_K$$

by projection on the second factor. We contend that the inverse image of $\tau_K(A^{K/k})_k$ contains $H_0 \cap [(A^{L/k})_k \times A_K]$.

$$H_0 \cap [(A^{L/k})_k \times A_K] \to \tau_K(A^{K/k})_k$$

From this it will be clear that the desired factor group is finite.

Since H_0 is contained in the graph of a homomorphism of $A^{L/k}$ into A, it is itself the graph of a homomorphism β of its projection B on the first factor into A. Furthermore, B is contained in $A^{L/k}$, is defined over K, and hence over k by Chow's theorem. By the universal property of the K/k-trace, there exists a commutative diagram

$$\begin{tikzcd} B \arrow[rr, "\beta"] \arrow[dr, "\beta'"'] & & A \\ & A^{K/k} \arrow[ur, "\tau_K"'] & \end{tikzcd}$$

with β' defined over k, and hence $\beta(B_k)$ is contained in $\tau_K(A^{K/k})_k$. This proves our contention, and concludes the proof of our proposition.

COROLLARY. *If Theorem 1 is true for L/k, then it is true for K/k, i.e. if $A_L/\tau_L(A^{L/k})_k$ is finitely generated, so is $A_K/\tau_K(A^{K/k})_k$.*

Proof. This is immediate from the proposition and the fact that we have an injection

$$0 \to A_K/[\tau_L(A^{L/k})_k \cap A_K] \to A_L/\tau_L(A^{L/k})_k.$$

Next, we show that we may extend the constant field.

PROPOSITION 2. *Let k^* be any extension of k which is independent of K, and let $K^* = Kk^*$. Let A be an abelian variety defined over K and let (B, τ) be its K/k-trace. Then*

$$A_K \cap \tau B_{k^*} = \tau B_k.$$

Proof. From the definition of the trace, it is clear that (B, τ) is also a K^*/k^*-trace of A. Our assertion is obvious if k^* is separable over k. Hence it suffices to deal with a finite purely inseparable extension k^* of k. The inclusion $\tau B_k \subset A_K \cap \tau B_{k^*}$ is obvious. Conversely, let b be a point of B_{k^*} such that τb is rational over K. If we knew that τ is regular, i.e. that it is birational biholomorphic between B and its image in A, then in view of the fact that τ is defined over K, we would see immediately that $\tau^{-1}\tau b$ is rational over k. As we do not know that τ is regular, we use Chow's regularity theorem, according to the standard technique of [2], Ch. 9. We can write $K = k(u)$ for suitable parameters u, and $A = A_u$, $\tau = \tau_u$. Let $u_1, \cdots, u_m$ be independent generic specializations of u over k. For m large, the map

$$x \to (\tau_{u_1}x, \cdots, \tau_{u_m}x)$$

of B into $A_{u_1} \times A_{u_2} \times \cdots \times A_{u_m}$ is regular, and thus biholomorphic between

B and its image. If τb is rational over K, then $(\tau_{u_1}b, \cdots, \tau_{u_m}b)$ is rational over $k(u_1, \cdots, u_m)$, hence b is rational over $k(u_1, \cdots, u_m)$, hence b is rational over that field. Since b is purely inseparable over k, and since $k(u_1, \cdots, u_m)$ is regular over k, it follows that b is rational over k. This concludes the proof.

COROLLARY. *If Theorem* 1 *is true for* K^*/k^*, *then it is true for* K/k.

Proof. The factor group $A_K/\tau B_k$ can be identified with a subgroup of $A_{K^*}/\tau B_{k^*}$.

Finally, it will be convenient to deal with the case where K is a function field of dimension 1 over k, i.e. the function field of a curve, and the next proposition shows that the reduction to this case is trivial.

PROPOSITION 3. *Let* $K \supset E \supset k$ *be a tower of fields such that* K *is regular over* E *and* E *regular over* k. *If Theorem* 1 *is true for* K/E *and* E/k, *then it is true for* K/k.

Proof. Let A be as in Theorem 1, an abelian variety defined over K. Let $(A^{K/E}, \tau_{K/E})$ be a K/E-trace of A, and $(A^{E/k}, \tau_{E/k})$ a E/k-trace of $A^{K/E}$. By the universal mapping property, there is a purely inseparable homomorphism $\beta\colon A^{E/k} \to A^{K/k}$ defined over k such that the following diagram is commutative:

$$\begin{tikzcd}
A & \\
A^{K/E} \arrow[u, "\tau_{K/E}"] & A^{K/k} \arrow[ul, "\tau_{K/k}"'] \\
A^{E/k} \arrow[u, "\tau_{E/k}"] \arrow[ur, "\beta"] &
\end{tikzcd}$$

All the homomorphisms τ are purely inseparable, and thus injective. We have

$$A_K \supset \tau_{K/E}(A^{K/E})_E \supset \tau_{K/E}\tau_{E/k}(A^{E/k})_k = \tau_{K/k}\beta(A^{E/k})_k.$$

If we assume that $(A^{K/E})_E$ is of finite type modulo $\tau_{E/k}(A^{E/k})_k$, it follows that A_K modulo $\tau_{K/k}\beta(A^{E/k})_k$ is also of finite type. But this last group is contained in $\tau_{K/k}(A^{K/k})_k$. We see therefore that it suffices to prove Theorem 1 for each step K/E and E/k of our tower.

It is well known and easy to show that one can always construct a tower $E_0 = k \subset E_1 \subset \cdots \subset E_n = K$ such that each step E_i/E_{i-1} is regular and of transcendence degree 1. This comes from the lemma of Bertini's theorem,

to the effect that if x, y are two elements of K, algebraically independent over k, and such that $y \notin K^p k$, then for all but a finite number of constants $c \in k$, K is regular over $k(x+cy)$. (Cf. [1], Ch. 6.) If k is finite, one needs a small additional argument. However, in view of Proposition 2, for our purposes, we may assume k infinite.

We have thus reduced the proof of Theorem 1 to the case where k is algebraically closed and K is of transcendence degree 1 over k, i. e. is the function field of a curve.

3. The weak Mordell-Weil Theorem. By a *global field* we shall mean a field K which is either

a function field over an algebraically closed constant field k (i. e. a finitely generated regular extension of k)

or *an algebraic number field of finite degree over the rationals.*

We refer to these as the *function field case* and *number field case* respectively. We let $\dim K$ be the transcendence degree of K over k in the function field case. It is the dimension of a model of K over k. Our aim is to prove Theorems 1 and 2. The results of § 2 (and eventually those of § 8) will be used only to deal with the function field case. The case of number fields is thus somewhat simpler to deal with.

Let m be a natural number prime to the characteristic of K. Let A be an abelian variety defined over K, and let A_m denote the group of points of order m on A, i. e. the kernel of $m\delta$. To prove Theorem 1 or 2, we may assume that all point of A_m are rational over K, because we may deal with the finite separable extension $K(A_m)$ of K instead of K itself. This is obvious in the case of number fields, and follows from Proposition 1 in the case of function fields.

In this section, we prove the weak Mordell-Weil theorem, namely: *If A is an abelian variety defined over a global field K, such that $A_m \subset A_K$, and such that* $\dim K = 1$ *in the function field case, then the factor group A_K/mA_K is finite.* We reproduce essentially word for word the proof given in [3]. Although we could have limited ourselves to making a reference to that paper, we prefer to make our treatment here as self-contained as possible.

We shall use only two elementary and well-known properties of K. To state them, we denote by $\{\mathfrak{p}\}$ the set of all finite primes of K (i. e. in the case of function fields with $\dim K = 1$, the set of points of a model of K/k,

rational over k, and in the case of number fields, the set of all finite primes). Our properties may then be stated as follows.

a.) Let S be a finite set of primes. Then there are only a finite number of abelian extensions of K of exponent m (i.e. such that $\sigma^m = 1$ for all automorphisms of the extension over K) which are unramified outside S.

b.) There exists a finite set S of primes such that for $\mathfrak{p} \notin S$, the abelian variety $A_{\mathfrak{p}}'$ obtained by reducing A modulo $\mathfrak{p}$ is non-degenerate.

For the reduction of varieties, we refer the reader to Shimura [7]. We recall that a reduction (or specialization) of an abelian variety is said to be non-degenerate if the specialized cycle has one component, with multiplicity 1, which is an abelian variety whose law of composition is obtained by specializing that of A. Property b.) may of course also be expressed by saying that in an algebraic system of varieties whose generic member is an abelian variety, almost all members of the system are also abelian varieties whose laws of composition are obtained by specializing that of the generic member. Here, the parameter variety is a model of K/k in the case of function fields, and is a so-called absolute curve in the case of number fields.

The following two lemmas achieve what we want. The first one ties up the factor group A_K/mA_K with the extension $K(1/m \cdot A_K)$ of K obtained by adjoining to K all points $y \in A$ such that $my \in A_K$. It is an abelian extension, whose automorphisms are induced by translations of A_m, in view of the fact that we assumed $A_m \subset A_K$. Indeed, if σ is in the Galois group G and $my = x \in A_K$ then $\sigma(my) = m\sigma y = x$, so that $\sigma y - y \in A_m$.

LEMMA 1. *The factor group A_K/mA_K is finite if and only if $K(1/m \cdot A_K)$ is a finite extension of K.*

Proof. One implication is obvious. Conversely, assume that $K(1/m \cdot A_K)$ is finite over K. We have a bilinear map

$$(A_K, G) \to A_m$$

obtained as follows. Let $x \in A_K$. Let y be such that $my = x$. We put $(x, \sigma) = \sigma y - y$. This element of A_m obviously does not depend on the y selected such that $my = x$. It is clear that (x, σ) is bilinear in x and σ. It is trivially verified that the right-hand kernel of our pairing is 1, while the left-hand kernel is precisely mA_K. The groups A_K/mA_K and G are therefore paired exactly into A_m. Since G and A_m are finite, it follows that A_K/mA_K is also finite.

To conclude the proof of the weak Mordell-Weil Theorem, there remains but to show that $K(1/m\cdot A_K)$ is finite over K. This follows from a.) and b.) and our second lemma.

LEMMA 2. *If* $\mathfrak{p}$ *is a prime such that* $A_{\mathfrak{p}}'$ *is non-degenerate, and* $\mathfrak{p}\nmid m$, *then* $K(1/m\cdot A_K)$ *is unramified over* K *at* $\mathfrak{p}$.

Proof. This being a local statement, we may go over to the completion $K_{\mathfrak{p}}$ of K with respect to $\mathfrak{p}$. In the function field case, $K_{\mathfrak{p}}$ is the power series field over k. *Let* $x\in A_k$. It suffices to show that $K_{\mathfrak{p}}(1/m\cdot x)$ is unramified over $K_{\mathfrak{p}}$. We use a prime to denote the reduction of objects modulo $\mathfrak{p}$. Let $\mathfrak{a}=(m\delta)^{-1}(x)$. Then $\mathfrak{a}'=(m\delta')^{-1}(x')$, since $A_{\mathfrak{p}}'$ is non-degenerate. All points in $(m\delta')^{-1}(x')$ occur with multiplicity 1, since $\mathfrak{p}\nmid m$, and are rational over a finite separable extension L' of $K_{\mathfrak{p}}'$. (Here, $K_{\mathfrak{p}}'$ is the residue class field, and in the function field case, we have $L'=K_{\mathfrak{p}}'=k$.) By a suitable form of Hensel's lemma [3], it follows that all points of $\mathfrak{a}$ are rational over the unramified extension of $K_{\mathfrak{p}}$ obtained by lifting L'. In the case of function fields, this unramified extension is of course $K_{\mathfrak{p}}$ itself.

The needed form of Hensel's lemma, as stated in [3], is the following. *Let* L *be complete under a discrete valuation, with residue class field* L'. *Let* $\mathfrak{a}$ *be a positive* 0*-cycle, in a projective space, say, rational over* L, *and let* P' *be a point of* $\mathfrak{a}'$ *which is rational over* L', *and of multiplicity* 1 *in* $\mathfrak{a}'$. *Then there is a unique point* P *in* $\mathfrak{a}$ *which specializes to* P', *and* P *is rational over* L. The proof is immediate, taking into account the uniqueness of the extension of the valuation to algebraic extensions of L.

4. Heights in function fields. In order to carry out the infinite descent in § 7, we need to be able to measure the size of a point rational over K, or as is customary to say, its height. It is convenient to give the definition of the height separately for the function field and number field case. We do this in this section and the next. The fundamental properties of heights are given in § 6, and there the statements and proofs can again be formulated uniformly for the two cases.

In this section, we assume that k is algebraically closed. Let W be a complete non-singular curve defined over k, and let $K=k(w)$ be a function field for W over k, (w) being a generic point of W over k. We follow [6] essentially without change.

We shall define the height of a point P in projective space $\boldsymbol{P}^n$, rational over K. Let $(y_0,\cdots,y_n)$ be a set of homogeneous coordinates for P, rational

over K. Then the y_i may be viewed as functions on W, defined over k. We define the *height of* P to be

$$h(P) = h(y) = -\deg \inf_i (y_i), \tag{1}$$

where (y_i) denotes as usual the divisor of y_i. Since the degree of the divisor of a function is equal to 0, we see on the one hand that $h(P)$ does not depend on the set of homogeneous coordinates representing P, and on the other hand that $h(P) \geqq 0$ (because we could take say $y_0 = 1$). Furthermore, $h(P) = 0$ if and only if P is rational over k, i. e. is constant.

One can give an alternate geometric definition of the height. Let $T(P)$, which we also write $T(y)$, be the locus of P over k. It is a curve, which may of course have singularities. We have a rational map $f\colon W \to \boldsymbol{P}^n$ such that that $f(w) = (y)$. It is induced by a surjective rational map of W onto $T(y)$. We contend that

$$h(y) = (\deg f) \deg T(y), \tag{2}$$

where $\deg f$ is the degree of the rational map of W onto $T(y)$ (non-zero if f is not constant), and $\deg T(y)$ is the projective degree of the variety $T(y)$. To prove this, we may assume without loss of generality that none of the y_i is 0, and that (y) is not constant. Let (Y) be the variables of $\boldsymbol{P}^n$, and let $H = H(Y)$ be a hyperplane defined over k, such that $T(y) \cdot H$ is defined. Put $z = H(y)$. Then for each i, y_i/z is an element of K, and thus a function on W. Furthermore, if we denote by H_i the divisor of the hyperplane $Y_i = 0$, then $H_i - H$ is the divisor of a function on $\boldsymbol{P}^n$, which can also be viewed as a function on $W \times \boldsymbol{P}^n$. Let Γ_f denote the graph of f. It is biholomorphic to W under projection on the first factor. Under this identification, it is clear that the function on $W \times \boldsymbol{P}^n$ whose divisor is $W \times (H_i - H)$ induces y_i/z on Γ_f. Hence by [10], F-VIII$_3$, Th. 4, Cor. 2, we get

$$(y_i/z) = f^{-1}(H_i) - f^{-1}(H).$$

By definition, we have

$$h(y) = -\deg \inf_i (y_i/z) = -\deg \inf_i [f^{-1}(H_i) - f^{-1}(H)].$$

Since the hyperplanes H_i have no point in common, neither do the divisors $f^{-1}(H_i)$ on W, and consequently, $h(y) = -\deg(-f^{-1}(H)) = \deg(f^{-1}(H))$. We have

$$h(y) = \deg[\Gamma_f \cdot (W \times H)]$$

since the degree of a 0-cycle does not change under projection. Projecting on the right, we have

$$h(y) = (\deg f)(\deg T(y) \cdot H)$$

which proves our contention.

From definition (2) of he height, we see that for $h(y)$ bounded, the degree of $T(y)$ is also bounded. Hence by the theory of Chow coordinates, we get our first property of heights.

PROPERTY 1F. *In the function field case, with* $\dim K = 1$, *let* (y) *be a point of* $\boldsymbol{P}^n$ *rational over* K. *Let* $T(y)$ *be the locus of* (y) *over* k. *If* $h(y)$ *is bounded, then* $\deg T(y)$ *is bounded, and* $T(y)$ *can belong only to a finite number of algebraic families.*

The definition of heights can also be given when $\dim W > 1$ [6]. In fact, let W be a projective normal model of K over k. If $P = (y)$ is again a point in $\boldsymbol{P}^n$, rational over K, we can define $h(P)$ as in (1), with the understanding that deg now denotes the projective degree of the divisor $\inf_i(y_i)$, in the given projective embedding of W. Thus if $\dim W > 1$, the height of P depends on the choice of model for K over k, while it does not if $\dim W = 1$. As in the case where $\dim W = 1$, we have

PROPOSITION 4. *Let* W *be a projective normal model of* K *over the algebraically closed field* k. *Let* $(y_0, \cdots, y_n)$ *be projective coordinates of a point* P *in* $\boldsymbol{P}^n$, *with* $y_i \in k(W) = K$. *Let* $T(P)$ *be the locus of* P *over* k, *and* $f \colon W \to \boldsymbol{P}^n$ *the corresponding rational map of* W *into* $\boldsymbol{P}^n$. *Then for a generic hyperplane* H *of* $\boldsymbol{P}^n$, *we have*

$$h(P) = -\deg \inf_i(y_i) = \deg f^{-1}(H).$$

Proof. The arguments follow exactly those given above for curves. The degree is the projective degree in the given projective embedding of W. One sees immediately that the projection on W of any subvariety of codimension 1 of Γ_f must be of codimension 1 on W, and hence simple on Γ_f since f is defined at such a subvariety. Thus W and Γ_f are biholomorphic at such a subvariety, and the arguments given above hold (especially [10], F-VIII$_3$, Th. 4, Cor. 2).

The analogue of (2) if $\dim W > 1$ could also be given, but we omit it. We do not need it for the proof of Theorem 1. We note that the properties of heights proved in § 6 depend only on definition (1).

When dealing simultaneously with the function field and number field

case, it is often convenient to replace the height as we have defined it in (1) by an exponential of it. Indeed, in number fields, the valuations are usually written multiplicatively because of the archimedean ones. To make arguments run completely parallel and to avoid a repetition of formulas in additive and multplicative notation, we therefore define the multiplicative height in function fields as follows. Let c be a number, $0 < c < 1$. We put

$$h^*(P) = c^{-h(P)} \tag{3}$$

and call this the *multiplicative height*, or simply height if it is used constantly throughout a section. Let $\dim W = 1$. For each point $\mathfrak{p}$ of W, rational over k, and a function $y \in K$, we define the absolute value $v_{\mathfrak{p}}$ as usual by

$$v_{\mathfrak{p}}(y) = c^{\operatorname{ord}_{\mathfrak{p}} y}, \tag{4}$$

where $\operatorname{ord}_{\mathfrak{p}} y$ is the order of the zero of y at $\mathfrak{p}$ (negative if y has a pole). Thus a function has a zero of high order at $\mathfrak{p}$ if $v_{\mathfrak{p}}(y)$ is close to 0, and a pole of high order at $\mathfrak{p}$ if $v_{\mathfrak{p}}(y)$ is large, close to $+\infty$.

In view of the — sign in (1) and the fact that $0 < c < 1$, we get by a trivial computation

$$h^*(P) = \prod_{\mathfrak{p}} \sup_i v_{\mathfrak{p}}(y_i). \tag{5}$$

It is this expression which is used to define the height in number fields, as we shall see in the next section. We note that $h^*(P) \geqq 1$.

If $\dim W > 1$, we shall say that $\mathfrak{p}$ is a *prime divisor of* K if it is a prime divisor of W, i. e. a subvariety of W of codimension 1, defined over k. Then $\deg \mathfrak{p}$ is the projective degree of $\mathfrak{p}$ in the given projective embedding of W, and $v_{\mathfrak{p}}(y)$ is defined by

$$v_{\mathfrak{p}}(y) = c^{(\deg \mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} y}.$$

Formula (5) is then clearly applicable without change.

5. Heights in number fields. Let K be a number field of finite degree over the rationals $\boldsymbol{Q}$. Let $\mathfrak{p}$ be a finite prime of K, corresponding to a prime ideal in its ring of integers. Let $N\mathfrak{p}$ be as usual the number of elements in the residue class field. For $y \in K$, we let

$$v_{\mathfrak{p}}(y) = (1/N\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}} y},$$

where $\operatorname{ord}_{\mathfrak{p}} y$ is the order of y at the discrete valuation of K determined by $\mathfrak{p}$.

If $\mathfrak{p}$ is an infinite prime, i. e. is a real or a pair of complex conjugate

embeddings of K into the complex numbers, then we let $v_{\mathfrak{p}}(y)$ be the ordinary absolute value if the embedding is into the reals, and the square of the ordinary absolute value if the embedding is not real. The product formula states that for $y \in K$, $y \neq 0$, we have

$$\prod_{\mathfrak{p}} v_{\mathfrak{p}}(y) = 1.$$

Let $(y_0, \cdots, y_m)$ be a set of homogeneous coordinates for a point P in $\boldsymbol{P}^m$, with $y_i \in K$. We define the *height* $h(P)$ of P by the relation

$$h(P)^{[K:\boldsymbol{Q}]} = \prod_{\mathfrak{p}} \sup_i v_{\mathfrak{p}}(y_i). \tag{6}$$

The product formula guarantees that this depends only on the point in projective space and not on the coordinates chosen. Since one of the y_i could have been chosen equal to 1, we see that $h(P) \geqq 1$. The extra term $[K: \boldsymbol{Q}]$ has been added to insure that $h(P)$ does not depend on the field K over which P is rational.

If σ is an automorphism of K over $\boldsymbol{Q}$, then by transport of structure, we have $h(P^\sigma) = h(P)$.

The (absolute) degree $d(P)$ of P is defined to be the degree $[K:\boldsymbol{Q}]$, where $K = \boldsymbol{Q}(P)$ is the field obtained by adjoining to $\boldsymbol{Q}$ a set of affine coordinates for P, say $y_1/y_0, \cdots, y_m/y_0$. We have the following strong version of Property 1F.

PROPERTY 1N. (Northcott) *Let h_0, d_0 be two fixed numbers. Then there is only a finite number of points P in $\boldsymbol{P}^m$ such that $d(P) \leqq d_0$ and $h(P) \leqq h_0$.*

Proof. Let us first consider the case where $d(P) = 1$, i.e. P is rational over $\boldsymbol{Q}$. Multiplying the y_i by a suitable integer, we may assume that all y_i are integers, and that their g.c.d. is equal to 1. For all finite primes p of $\boldsymbol{Q}$, we then get $\sup_i v_p(y_i) = 1$. The height of P is then determined by the ordinary absolute value, and the result is obvious.

We prove the property in general by reducing it to the preceding case. Let $(T_0, \cdots, T_m)$ be variables. Let

$$F(T) = \sum x_\alpha M_\alpha(T)$$

be a form in the T's, where the M_α are monomials, whose coefficients x_α lie in a number field. Then (x) may be viewed as a point in some projective space $\boldsymbol{P}^N$. We define the *height of F* to be the height of (x), and write it $h(F)$.

LEMMA. *Let d_1, d_2 be two natural numbers. Then there exists a number s depending only on d_1, d_2 such that if F_1, F_2 are two forms of degrees d_1, d_2 respectively with coefficients in a number field K, then*

$$h(F_1F_2) \leqq sh(F_1)h(F_2).$$

Proof. Let $F_1 = \sum x_\alpha M_\alpha(T)$ and $F_2 = \sum y_\beta M_\beta(T)$. Put $F_1F_2 = \sum z_\lambda M_\lambda(T)$. Then

$$z_\lambda = \sum x_{\alpha(\lambda)} y_{\beta(\lambda)},$$

where $\alpha(\lambda)$, $\beta(\lambda)$ range over those indices α, β such that $M_{\alpha(\lambda)}M_{\beta(\lambda)} = M_\lambda$. If $\mathfrak{p}$ is a finite prime of K, then obviously

$$v_\mathfrak{p}(z_\lambda) \leqq \sup_\alpha v_\mathfrak{p}(x_\alpha) \sup_\beta v_\mathfrak{p}(y_\beta),$$

and hence we can add a $\sup_\lambda$ to the left hand side of this inequality.

If $\mathfrak{p}$ is archimedean, then there obviously exists an integer $s_\lambda(d_1, d_2)$ such that

$$v_\mathfrak{p}(z_\lambda) \leqq s_\lambda(d_1, d_2) \sup_\alpha v_\mathfrak{p}(x_\alpha) \sup_\beta v_\mathfrak{p}(y_\beta).$$

This $s_\lambda(d_1, d_2)$ is the number of terms in the sums expressing z_λ in terms of $x_{\alpha(\lambda)}y_{\beta(\lambda)}$, or its square if $\mathfrak{p}$ is complex. Hence there exists an integer $s(d_1, d_2)$ such that

$$\sup_\lambda v_\mathfrak{p}(z_\lambda) \leqq s(d_1, d_2) \sup_\alpha v_\mathfrak{p}(x_\alpha) \sup_\beta v_\mathfrak{p}(y_\beta).$$

Taking the product over all $\mathfrak{p}$, we get

$$h(z)^{[K:Q]} \leqq s(d_1, d_2)^r h(x)^{[K:Q]} h(y)^{[K:Q]},$$

with an integer $r \leqq [K:\boldsymbol{Q}]$. This proves our lemma.

To conclude the proof of Property 1N, let $(y_0, \cdots, y_m)$ be a point of degree d_0, with say $y_0 = 1$. Let

$$F(T) = \prod_\sigma (y_0{}^\sigma T_0 + \cdots + y_m{}^\sigma T_m)$$

the product being taken over all conjugates of the field $\boldsymbol{Q}(y)$, so that $F(T)$ is of degree d_0. We call $F(T)$ the *Chow form* of $P = (y)$. It is clear that two points have the same Chow form if and only if they are conjugate over $\boldsymbol{Q}$, because $F(T)$ factorizes essentially uniquely. Hence by the lemma, we get

$$h(F) \leqq s(d_0) h(P)^{d_0}, \tag{7}$$

where $s(d_0)$ is an integer depending only on d_0, and not on P. Our property is obvious from this relation, the first paragraph of the proof, and the fact that $h(P) = h(P^\sigma)$.

6. Properties of heights. Let K be a global field, and let V be an abstract variety defined over K. Let λ, λ' be two real-valued functions on V_K (the rational points of V in K). We shall say that they are *equivalent*, and write $\lambda \sim \lambda'$, if there exist two real numbers $c_1, c_2 > 0$ such that for all $P \in V_K$, we have

$$c_1\lambda(P) \leqq \lambda'(P) \leqq c_2\lambda(P).$$

This equivalence relation will be applied to heights. In this section and the next, the height is taken to be multiplicative in the function field case, and we write h instead of h^*. (If it were taken additive, as in (1), then we would make the above relation read

$$c_1 + \lambda(P) \leqq \lambda'(P) \leqq c_2 + \lambda(P)$$

and we would omit the condition $c_1, c_2 > 0$.)

Actually, we remark (as in [8]) that in number fields, we can consider the stronger equivalence relation where λ, λ' are functions on all absolutely algebraic points of V, the constants working uniformly for all such points. All the statements which we shall make concerning the equivalence of heights in the sequel are valid under this stronger interpretation. If we adopted a device in function fields analogous to the one in number fields, i. e. once K is fixed, define the height for points rational over the algebrais closure $\bar{K}$ of K by taking suitable roots, then a similar remark would apply in function fields.

Let now V be a complete, abstract, normal variety defined over K. Let $\phi\colon V \rightarrow \boldsymbol{P}^m$ be an everywhere defined rational map of V into projective space, defined over K. Then for each point P of V_K, $\phi(P)$ is a point of $\boldsymbol{P}^m$, rational over K, and we can thus define its height, which we shall denote by $h_\phi(P)$. We shall give below conditions under which the real-valued functions h_ϕ are equivalent. As mentioned before, the properties of heights in the case of function fields depend only on definition (1) or (3), and for the proof of Theorem 1, are needed only in the case $\dim K = 1$.

It follows immediately from the definition of the height that if ϕ' is another rational map of V into $\boldsymbol{P}^m$ which differs from ϕ by a projective transformation defined over K, then $h_\phi \sim h_{\phi'}$. Indeed, the elements of K which enter into such a transformation can introduce only a uniformly bounded change in the height of a point because they are fixed once for all.

We shall obtain mappings $\phi\colon V \rightarrow \boldsymbol{P}^m$ by means of linear systems. Let $\mathfrak{L}$ be a linear system on V, defined over K. This means that we can find a divisor $X_0 \in \mathfrak{L}$, rational over K, such that the space of functions L_0 con-

sisting of all functions on V whose divisors are of type $X - X_0$ with $X \in \mathfrak{L}$ has a basis defined over K. If $(f_0 = 1, \cdots, f_m)$ is such a basis, then it defines a rational map $\phi: V \rightarrow \boldsymbol{P}^m$. If $\mathfrak{L}$ is without fixed point, then ϕ is everywhere defined ([1], Ch. 6). In view of the remark in the preceding paragraph, we see that the equivalence class of h_ϕ actually depends only on the linear system.

Let $\mathfrak{M}$ be another linear system on V, also defined over K. Then we can define the sum $\mathfrak{L} + \mathfrak{M}$ as a linear system in the usuall manner. If $(f_0 = 1, \cdots, f_m)$ is a basis for L_0 over K, and $(g_0 = 1, \cdots, g_n)$ is a basis for M_0 over K obtained in a similar manner, then we get a vector space of functions N_0 generated by the products $f_i g_j$. We have $f_0 g_0 = 1$. The divisor of $f_i g_j$ is $(f_i g_j) = (f_i) + (g_j)$. If we write $(f_i) = X_i - X_0$ and $(g_j) = Y_j - Y_0$ then $(f_i g_j) = X_i + Y_j - (X_0 + Y_0)$. The space N_0 gives rise to a linear system $\mathfrak{N}$ called the sum of $\mathfrak{L}$ and $\mathfrak{M}$. If $\mathfrak{L}$ and $\mathfrak{M}$ are both without fixed points, so is $\mathfrak{L} + \mathfrak{M}$.

Let $\phi: V \rightarrow \boldsymbol{P}^m$ and $\psi: V \rightarrow \boldsymbol{P}^n$ be two rational maps derived from $\mathfrak{L}$ and $\mathfrak{M}$. The functions $\{f_i g_j\}$ give rise to a rational map η of V into $\boldsymbol{P}^{(m+1)(n+1)-1}$. If we denote by $\phi + \psi$ any one of the rational maps (defined over K) derived from $\mathfrak{L} + \mathfrak{M}$, and determined only up to a projective transformation, then obviously, $h_\eta = h_\phi h_\psi$ and $h_\eta \sim h_{\phi+\psi}$. Summarizing, we get

PROPERTY 2. *Let V be a complete, abstract, normal variety defined over K. Let $\mathfrak{L}$, $\mathfrak{M}$ be two linear systems on V, also defined over K, and without fixed points. Let ϕ, ψ be two rational maps of V into $\boldsymbol{P}^m$, $\boldsymbol{P}^n$ respectively, defined by these systems over K, and let $\phi + \psi$ be a rational map defined over K by $\mathfrak{L} + \mathfrak{M}$. Then $h_{\phi+\psi} \sim h_\phi h_\psi$.*

The next property also follows immediately from the definitions.

PROPERTY 3. *Let U, V be two complete, abstract varieties defined over K. Assume U normal and V non-singular. Let $\omega: U \rightarrow V$ be an everywhere defined, surjective rational map, defined over K. Let $\mathfrak{L}$ be a linear system on V, defined over K, and let $\omega^{-1}(\mathfrak{L})$ be the linear system on U consisting of all divisors $\omega^{-1}(X)$ as X ranges over $\mathfrak{L}$. Let ϕ be a rational map of V into $\boldsymbol{P}^m$ defined by $\mathfrak{L}$ over K. Then $\phi \circ \omega$ is a rational map associated with the linear system $\omega^{-1}(\mathfrak{L})$. Assume in addition that $\mathfrak{L}$ is without fixed points. Then so is $\omega^{-1}(\mathfrak{L})$, and we have*

$$h_{\phi \circ \omega} = h_\phi \circ \omega.$$

Proof. We have assumed V non-singular in order to insure that the

inverse image of a divisor linearly equivalent to 0 is also linearly equivalent to 0 (cf. [2], App. 1). That $\omega^{-1}(\mathfrak{L})$ is then a linear system is obvious, and so is the rest of our assertions.

The preceding three properties of heights have been trivial consequences of the definitions. Our fourth and last property, although not difficult to prove, will require a slightly more elaborate argument. We have taken it and its proof from Weil's paper [8].

PROPERTY 4. *Let V, $\mathfrak{L}$, $\mathfrak{M}$, ϕ, ψ be as in Property 2. If the divisors of $\mathfrak{L}$ and $\mathfrak{M}$ are linearly equivalent to each other, then $h_\phi \sim h_\psi$.*

Proof. In the course of the proof we shall use frequently the fact that if a function $f \in K(V)$ is not defined at a point Q of V, then it has a pole passing through Q ([1], Ch. 6) and hence if there exists a place of $K(V)$ over K which maps f on ∞ (resp. on 0), then f has a pole (resp. a zero) passing through Q.

By transitivity, we may clearly assume that $\mathfrak{M}$ is the complete linear system containing $\mathfrak{L}$.

Let X_0 be as before a divisor of $\mathfrak{L}$, rational over K, such that the derived space of functions L_0 has a basis $(f_0, \cdots, f_m)$ defined over K. For each f_i we can write

$$(f_i) = X_i - X_0.$$

We denote by ϕ_i the rational map of V into the affine K-open subset of $\boldsymbol{P}^m$ determined by the functions $(f_0/f_i, \cdots, f_m/f_i)$. We let V_i be the K-open subset $V - \operatorname{supp}(X_i)$ of V. Then the V_i cover V, and ϕ_i is defined at every point of V_i.

In view of our assumption on $\mathfrak{M}$, we may take $Y_0 = X_0$ and $M_0 = L(X_0)$. Let $(g_0, \cdots, g_n)$ be a basis of $L(X_0)$ defined over K, and put

$$(g_j) = Y_j - X_0.$$

We may assume that $g_i = f_i$ $(i = 0, \cdots, m)$. We have a rational map ψ_j of V into the affine K-open subset of $\boldsymbol{P}^n$ determined by $(g_0/g_j, \cdots, g_n/g_j)$, and ψ_i is defined at every point of V_i for $i = 0, \cdots, m$. Thus to compute $h_\psi(P)$ for $P \in V_K$, we may restrict ourselves to $h_{\psi_i}(P)$ for $P \in V_i \cap V_K$.

Consider first the points of V_K which are in V_0. Let g be any one of the g_j $(j = 0, \cdots, n)$. We contend that the ideal generated by $(f_0/g, \cdots, f_m/g)$ in the ring $K[f_0/g, \cdots, f_m/g]$ is the unit ideal. Otherwise, it is contained in a maximal ideal, and there is a place of the function field $K(V)$ over K which maps all f_i/g on 0. This place induces a point Q on V, and hence

the functions f_i/g must all have a zero passing through Q. Since $(f_i/g) = X_i - Y$ with $Y > 0$, this implies that $Q \in \operatorname{supp}(X_i)$ for all i, and contradicts our assumption that they have no point in common.

From the above, we can write

$$1 = \sum z_\nu \boldsymbol{M}_\nu(f_i/g)$$

with $z_\nu \in K$. Here, $\boldsymbol{M}_\nu$ stands for a monomial $(f_0/g)^{\nu_0} \cdots (f_m/g)^{\nu_m}$. Note that the z_ν do not depend on $P \in V$, and that $\deg \boldsymbol{M}_\nu \geqq 1$.

Put $x_i = f_i(P)$, where P is any point in V_0, and $y = g(P)$. Suppose first that $y \neq 0$. Then

$$1 = \sum z_\nu \boldsymbol{M}_\nu(x_i/y).$$

For every prime $\mathfrak{p}$ of K, it follows that there exists a number $c_\mathfrak{p} > 0$ which is equal to 1 for all but a finite number of $\mathfrak{p}$, such that

$$\sup_i v_\mathfrak{p}(x_i/y) \geqq c_\mathfrak{p}.$$

(In function fields, this means that there exists a finite set S of prime divisors of W such that the x_i/y cannot have a common zero for $\mathfrak{p} \notin S$, and that for $\mathfrak{p} \in S$, the order of such a common zero cannot be arbitrarily high. The set S can be taken to be the set where some z_ν has a pole.)

Since we selected g arbitrarily among the g_j, we get

$$\sup_i v_\mathfrak{p}(x_i) \geqq c_\mathfrak{p} \sup_j v_\mathfrak{p}(y_j),$$

where $y_j = g_j(P)$. We emphasize that $c_\mathfrak{p}$ depends only on the z_ν, and not on $P \in V_0 \cap V_K$. Furthermore, this formula clearly holds whether $y_j = 0$ or not, i. e. for all P in $V_0 \cap V_K$. Taking the product, we see that there exists a number $c_1 = c_1(V_0) > 0$ such that for all $P \in V_0 \cap V_K$ we have

$$c_1 h_\psi(P) \leqq h_\phi(P).$$

By symmetry, using the same arguments as above, there exists a constant $c_2 > 0$ such that for all $P \in V_0 \cap V_K$, we have

$$c_1 h_\psi(P) \leqq h_\phi(P) \leqq c_2 h_\psi(P).$$

Since V is covered by the finite number of K-open sets $V_0, \cdots, V_m$, we can repeat the above procedure for each one of them. We thus obtain numbers $c_1(V_i)$ and $c_2(V_i)$. In the statement of our property, we simply take the smallest of the former and the largest of the latter to conclude the proof.

7. The infinite descent. Let K be a global field, and let A be an abelian variety embedded in a projective space $\boldsymbol{P}^n$ over K. The height of a point $P \in A_K$ determined by the identity mapping of A into $\boldsymbol{P}^n$ is denoted by $h(P)$. In the function field case, we deal with the multiplicative height.

Let $m > 1$ be a natural number such that A_K/mA_K is finite, and let $a_1, \cdots, a_s$ be representatives of A_K/mA_K. Then any point P in A_K is congruent to some a_i mod mA_K. Denote by S a sequence $\{P_0, P_1, \cdots\}$ of points of A_K, constructed by starting with an arbitrary point P_0, and such that

$$mP_{\nu+1} = P_\nu - a_{i_\nu}.$$

We contend that there is a number $c_1 > 0$ independent of S, and an integer $\nu(S)$ depending on S such that for any sequence S, we have $h(P_\nu) \leqq c_1$ for $\nu > \nu(S)$. This contention is an obvious consequence of the fact, to be proved below, that there exists a number $c_2 > 0$ independent of S such that

$$h(P_{\nu+1})^{m^2-1} \leqq c_2 h(P_\nu). \tag{8}$$

Actually, we shall prove

PROPOSITION 5. *Let K be a global field. Let A be an abelian variety embedded in projective space $\boldsymbol{P}^n$ over K. Let $m > 1$ be a natural number, and let $a \in A_K$. Then there exists a number $c_2(a, m)$ depending on a and on m, such that for any $P \in A_K$, we have*

$$h(P)^{m^2-1} \leqq c_2(a, m) h(mP + a).$$

To deduce (8) from Proposition 5, we let a range over the a_i, and let $c_2 = \sup_i c_2(a_i)$.

From the manner in which the sequences are constructed, we see that for each ν, there exist integers $n_1, \cdots, n_s$ such that

$$P_0 = m^\nu P_\nu + n_1 a_1 + \cdots + n_s a_s$$

and we obtain the pay-off of our infinite descent.

COROLLARY. *Let m be such that A_K/mA_K is finite, and let $a_1, \cdots, a_s$ be representatives in A_K of A_K/mA_K. There exist a number c_1 and a subset $\mathfrak{S}$ of A_K such that:*

(i) *$h(P) \leqq c_1$ for all $P \in \mathfrak{S}$, and*

(ii) *for any $P_0 \in A_K$, there exist integers $n_0, n_1, \cdots, n_s$ and a point $P \in \mathfrak{S}$ such that*

$$P_0 = n_0 P + n_1 a_1 + \cdots + n_s a_s.$$

In the case of number fields, we apply Property 1N to conclude the proof of Theorem 2. The case of function fields will require an additional argument, which will be supplied in the next and final section.

We observe that A_K/mA_K was proved finite in § 3 only for a special case of K. A posteriori, once Theorems 1 and 2 are proved, one sees of course that A_K/mA_K is finite for all global fields.

Let us now prove Proposition 5. Let a be a point of A_K. Let $\omega\colon A \to A$ be the rational map $\omega u = mu + a$. Let X be a hyperplane section of A in its given projective embedding, rational over K. From now on we use constantly the results and notations of [2], Ch. 5 concerning divisors on abelian varieties. Aside from those, we use only Properties 2, 3, 4 of heights. To begin with, we have immediately from the definitions

$$\omega^{-1}(X) = (m\delta)^{-1}(X_{-a}) = (m\delta)^{-1}(X_{-a} - X) + (m\delta)^{-1}(X).$$

We also have

$$(m\delta)^{-1}(X) \equiv m^2 X,$$

this being deeper. One knows that the equivalence $\equiv$ is the same as algebraic equivalence. (This uses the fact that there is no torsion, not proved in [2]. Using only what is proved there, namely that it is the same as the torsion equivalence, we could dispense with this, at the cost of introducing in an obvious manner a multiple of the equivalences below.) Since X is a hyperplane section, the homomorphism $u \to \mathrm{Cl}(X_u - X)$ of A into $\hat{A}$ is surjective. Hence there is a point b of A such that

$$(m\delta)^{-1}(X) - m^2 X \sim X_b - X.$$

Furthermore, for the same reason, there exists a point $c \in A$ such that $(m\delta)^{-1}(X_{-a} - X) \sim X_c - X$. Thus we get finally

$$\begin{aligned} \omega^{-1}(X) &\sim X_c - X + m^2 X + X_b - X \\ &\sim m^2 X + X_d - X \\ &\sim (m^2 - 1)X + X_d \end{aligned}$$

with $d = b + c$. Now d is not necessarily rational over K, but since X is ample, so is X_d. Since $\omega^{-1}(X) - (m^2 - 1)X$ is linearly equivalent to an ample divisor over some field, and is itself rational over K, we conclude that there exists an ample positive divisor X' rational over K such that

$$\omega^{-1}(X) \sim (m^2 - 1)X + X'. \tag{9}$$

The divisors in the complete linear system containing $\omega^{-1}(X)$ are linearly

equivalent to the divisors of the sum of the complete linear systems containing $(m^2-1)X$ and X'. If $Y>0$ is a divisor on A rational over K, whose complete linear system $\mathfrak{L}(Y)$ is without fixed point, we select a definite rational map ϕ_Y defined over K, associated with $\mathfrak{L}(Y)$, in the class of such mappings determined only up to a projective transformation. We shall write h_Y instead of h_{ϕ_Y}. From (9) and Properties 2 and 4 we get

$$h_{\omega^{-1}(X)} \sim h_X{}^{(m^2-1)} h_{X'}.$$

Also by Property 4, we have $h \sim h_X$. (The linear system of hyperplane sections in the given embedding of A in $\boldsymbol{P}^n$ might not be complete, so we cannot write an equality.) Hence by Property 3 and 4 we see that there exists a number $c_2 = c_2(a, m)$ such that

$$h(P)^{m^2-1} h_{X'}(P) \leqq c_2 h(\omega(P)).$$

From the definition of the height (multiplicative in function fields), we know that $h_{X'}(P) \geqq 1$ for all $P \in A_K$. Hence

$$h(P)^{m^2-1} \leqq c_2 h(mP+a).$$

This concludes the proof of Proposition 5, and of Theorem 2.

8. End of the proof of Theorem 1. We consider the function field case. We let $W \subset \boldsymbol{P}^r$ be a projective, normal variety defined over the algebraically closed field k. Let w be a generic point of W over k, and $K = k(w)$ a function field for W over k. Let A be an abelian variety defined over K, and embedded in projective space $\boldsymbol{P}^n$ over K. Let u be a generic point of A over K. We shall denote by $W \circ A$ the locus of (w, u) over k. Then $W \circ A$ is the graph of the algebraic family parametrized by W, of which A is a generic member. (If we put $Z = W \circ A$, then $A = Z(w) = \mathrm{pr}_2[Z \cdot (w \times \boldsymbol{P}^n)]$.)

Given a rational point P of A over K, we shall denote by W_P the locus of (w, P) over k. Then

$$W_P \subset W \circ A \subset W \times \boldsymbol{P}^n \subset \boldsymbol{P}^r \times \boldsymbol{P}^n.$$

Note that W_P and W are birationally equivalent under the projection pr_1 (biholomorphic if W is a curve).

There is a projective embedding $\phi: \boldsymbol{P}^r \times \boldsymbol{P}^n \to \boldsymbol{P}^{(r+1)(n+1)-1}$ which to each products of points with homogeneous coordinates $(x_0, \cdots, x_r) \times (y_0, \cdots, y_n)$ assigns the point with homogeneous coordinates $(x_i y_j)$. One verifies immediately that for any $P \in A_K$, we have

$$h_\phi(w, P) \leqq h(w) + h(P) = \deg W + h(P).$$

Assume $\dim K = 1$. If $\mathfrak{S}$ is a subset of A_K such that $h(P) \leqq c_3$ (the constant of the corollary to Proposition 5), then by Property 1F, there exists a constant c_4 such that $\deg \phi(W_P) \leqq c_4$, and hence W_P can belong only to a finite number of algebraic families on $W \circ A$ for $P \in \mathfrak{S}$. In view of the corollary to Proposition 5, we shall be through with the proof of Theorem 1 once we have proved

THEOREM 3. *Let W be a projective, normal variety defined over the algebraically closed field k. Let w be a generic point of W over k, and $K = k(w)$ a function field of W over k. Let A be an abelian variety defined over K, and let (B, τ) be its K/k-trace. For each point $P \in A_K$, let W_P be the locus of (w, P) over k. If P, $P' \in A_K$ are such that W_P and $W_{P'}$ are in the same algebraic family on $W \circ A$, then P and P' are congruent modulo ${}_\tau B_k$* (i.e. $P - P' \in {}_\tau B_k$).

Proof. We shall prove our theorm by going from W_P to $W_{P'}$ by passing through a generic member of the family. Our first step is to show that a generic member is of the same type as W_P.

LEMMA. *Let U be a subvariety of $W \circ A$, defined over an extension k^* of k, independent of K over k, and such that W_P is a specialization of U over k. Put $K^* = Kk^*$. Then there exists a rational point P^* of A in K^* such that $U = W_{P^*}$.*

Proof. We have $\mathrm{pr}_1 W_P = W$. Hence by the compatibility of projections with specializations [4], we must have $\mathrm{pr}_1 U = W$. But $\dim U = \dim W$, and hence a generic point of U over k^* is of type (w, Q) for some $Q \in \boldsymbol{P}^n$, algebraic over $k^*(w)$. We must show that Q is rational over $k^*(w)$, and that Q is in A.

On $W \times \boldsymbol{P}^n$ the intersection $U \cdot (w \times \boldsymbol{P}^n)$ is obviously defined, and in view of the above remarks, we have

$$U \cdot (w \times \boldsymbol{P}^n) = \sum_{i=1}^{d} (w, Q_i)$$

for suitable points Q_i. Taking the projection on W, we see immediately that $d = 1$. Since $U \cdot (w \times \boldsymbol{P}^n)$ is rational over $k^*(w)$, so is $Q_1 = P^*$. Finally, we have $P^* \in A$ because

$$w \times P^* = U \cdot (w \times \boldsymbol{P}^n) \subset (W \circ A) \cdot (w \times \boldsymbol{P}^n) = w \times A.$$

Note that in the lemma, we have made no use of the fact that A is an abelian variety: The same statement holds for any algebraic system of varieties.

It will suffice to prove Theorem 3 for W_P and W_{P^*}. Indeed, given W_P and $W_{P'}$ as in the theorem, there exists a subvariety W_{P^*} of $W \circ A$, defined over some k^*, such that both W_P and $W_{P'}$ are specializations of W_{P^*}. If $P - P^* \in {}_T B_{k^*}$ and $P' - P^* \in {}_T B_{k^*}$, then $P - P' \in {}_T B_{k^*}$, and by Proposition 2, $P - P' \in {}_T B_k$.

The field k^* may also be assumed to be of transcendence degree 1 over k, i. e. the parameter variety in the algebraic system joining W_P to W_{P^*} may be assumed to be a curve, by blowing up the point corresponding to W_P on the given parameter variety joining W_P and W_{P^*}. Algebraically speaking, there exists a field $k_1 \supset k$, a complete non-singular curve T defined over k_1, a generic point t^* of T over k_1, and a point t of T, rational over k_1, such that if we put $k^* = k_1(t^*)$, the variety W_{P^*} is defined over k^*, and W_P is the unique specialization of W_{P^*} over $t^* \to t$ (relative to k_1) [4]. Without loss of generality for the proof of Theorem 3, we may let $k = k_1$ (using once more Proposition 2). We have the following diagram of fields:

$$\begin{tikzcd}[column sep=small] & K^* = k^*(w) \arrow[dl, dash] \arrow[dr, dash] & \\ K = k(w) \arrow[dr, dash] & & k^* = k(t^*) \arrow[dl, dash] \\ & k & \end{tikzcd}$$

Let $\mathrm{Alb}(T)$ be the Albanese variety of T, defined over k, and let $f\colon T \to \mathrm{Alb}(T)$ be a canonical map, defined over k. Let $g\colon T \to A$ be the rational map defined over K by the expression $g(t^*) = P^*$. Then there is a homomorphism $\alpha\colon \mathrm{Alb}(T) \to A$ and a point $a \in A$ such that the following diagram is commutative.

$$\begin{tikzcd} T \arrow[r, "f"] \arrow[d, "g"'] & \mathrm{Alb}(T) \arrow[dl, "\alpha + a"] \\ A & \end{tikzcd}$$

By the definition of the K/k-trace, there exists a homomorphism $\beta\colon \mathrm{Alb}(T) \to B$ defined over k such that the following diagram is commutative.

$$\begin{tikzcd} & \mathrm{Alb}(T) \arrow[dl, "\alpha"'] \arrow[d, "\beta"] \\ A & B \arrow[l, "\tau"] \end{tikzcd}$$

Since t is simple on T, f is defined at t. Furthermore, since W_P is the unique specialization of W_{P^*} over $t^* \to t$ (relative to k or K), it follows that P is the unique specialization of P^* over $t^* \to t$ (relative to K). Hence $g(t) = P$, and

$$\begin{aligned} P^* - P = g(t^*) - g(t) &= \alpha f(t^*) + a - \alpha f(t) - a \\ &= \tau\beta f(t^*) - \tau\beta f(t) \\ &= \tau b \end{aligned}$$

with $b = \beta[f(t^*) - f(t)] \in B_{k^*}$. QED.

PARIS.

REFERENCES.

[1] S. Lang, *Introduction to algebraic geometry*, Interscience Publishers, New York, 1958.

[2] ———, *Abelian varieties*, Interscience Publishers, New York, 1958.

[3] S. Lang and J. Tate, "Principal homogeneous spaces over abelian varieties," *American Journal of Mathematics*, vol. 80 (1958), pp. 659-684.

[4] T. Matsusaka, "Specialization of cycles on a projective model," *Memoirs of the College of Science*, University of Kyoto, Series A, vol. 26, No. 2 (1950), pp. 167-173.

[5] A. Neron, "Problèmes arithmétiques et géometriques rattachés a la notion de rang courbe algébrique dans un corps," *Bulletin de la Societe Mathematique de France*, vol. 80 (1952), pp. 101-166.

[6] ———, "Arithmétique et classes de diviseurs sur les variétés algébriques," *Proceedings of the International Symposium on Algebraic number theory*, Tokyo-Nikko, 1955, pp. 139-154.

[7] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[8] A. Weil, "Arithmetic on algebraic varieties," *Annals of Mathematics*, vol. 53 (1951), pp. 412-444.

[9] ——, "Sur les criteres d'équivalence en géometrie algébrique," *Mathematische Annalen*, vol. 128 (1954), pp. 95-127.

[10] ———, Foundations of Algebraic Geometry. New York, 1946.

ON GROUPS OF MEASURE PRESERVING TRANSFORMATIONS. I.*

By H. A. DYE.[1]

1. Introduction. This study concerns the classification of automorphism groups of a finite non-atomic measure algebra, the object being the description of equivalence classes of groups under certain rather pervasive notions of equivalence. In essence, these are the following. Given a group G of measure preserving automorphisms α of the finite non-atomic measure algebra (M, λ), one considers those automorphisms α of (M, λ) which depend locally on G, or more precisely, which have a representation

$$\alpha(P) = \sum_n Q_n \alpha_n(P), \tag{1.1}$$

where the α_n are elements of G, the Q_n are mutually disjoint elements of M, and $\sum$ denotes the least upper bound in (M, λ). The collection of all automorphisms of (M, λ) which depend locally on G forms a group $[G]$ containing G, called the full group determined by G. Two groups G_1 and G_2 are called equivalent if they determine the same full group, and weakly equivalent if there exists an isomorphism φ between the algebras on which they act such that G_1 and $\varphi^{-1}G_2\varphi$ are equivalent. The effect of these equivalence concepts is to erase many distinctions of significance in traditional ergodic theory; for example, it develops that any two singly-generated ergodic automorphism groups acting on separable non-atomic measure algebras are weakly equivalent. Attention shifts, rather, to the local properties of automorphism groups: given a group G and an element P of M, we denote by $[G]_P$ the local subgroup of $[G]$ consisting of all automorphisms in $[G]$ which act as the identity off P, and say that a property of G is local if its validity for $[G]_P$ entails its validity for $[G]_{\bar{P}}$, where $\bar{P}$ denotes the smallest G-invariant element of M containing P. Three basic local properties are analyzed in this paper, concepts of type (I and II), and a concept of approximate finiteness.

Any automorphism group G splits as the direct sum of a group of type I and a group of type II. Groups of type I are uniquely decomposable, up to equivalence, into direct sums of freely-acting cyclic groups of finite order. Groups of type II—by definition, those with no type I summands—comprise,

* Received April 7, 1958.

[1] This research was supported in part by a National Science Foundation grant.

therefore, the interesting class. These abound in practice, any freely-acting infinite group being of type II, and are presumably highly ramified under equivalence. The heuristic viewpoint is that "type II" embraces a class of local properties, each strong enough to assure weak equivalence of all groups possessing such a property and having isomorphic fixed algebras (this, under appropriate homogeneity assumptions). Unfortunately, approximate finiteness, which we discuss below, is the only such local property known at present. And because implications of this property are not yet fully understood—the question arises, for example, if the approximate finiteness of a group does not depend on its algebraic structure alone, and not on its specific realizations as automorphism groups—further detailed study of approximate finiteness seems desirable for clues on the general type II structure.

By definition, an automorphism group G of (M, λ) is approximately finite if elements in each finite subset of G can be approximated simultaneously by elements in a finite subgroup of $[G]$. More precisely, given an arbitrary finite subset $\alpha_1, \cdots, \alpha_n$ of G and an $\epsilon > 0$, one requires that there exist a finite subgroup K of $[G]$ and elements $\alpha'_1, \cdots, \alpha'_n$ of K such that $\alpha_i(P) = \alpha'_i(P)$, for all P dominated by some E_i in M with $\lambda(I - E_i) < \epsilon$. A basic theorem in the subsequent development asserts that any countably generated approximately finite group is equivalent to a direct product of finite cyclic groups; and an alternative presentation of the theory can be made in which this statement serves as initial definition. Our main results on approximately finite groups are the following: any singly generated automorphism group is approximately finite (Theorem 1); any subgroup of an approximately finite group is approximately finite (Theorem 2); if M is countably generated over the fixed algebra Z of an automorphism group G, then G contains a maximal approximately finite subgroup with fixed algebra Z (Theorem 4); and finally, under certain countability assumptions, two approximately finite groups of type II are weakly equivalent if and only if they have isomorphic fixed algebras (Theorem 5). The existence of non-approximately finite groups is established by example in Section 8.

It will be evident to the specialist in operator theory that these results, after Theorem 2, correspond precisely to main theorems in the Murray-von Neumann-Kaplansky theory of approximately finite W^*-algebras of type II (see [2], [5], [8]). The present theory evolved, in fact, from a study of regular maximal abelian W^*-subalgebras of finite W^*-algebras, in the course of which this measure theoretic prototype of such algebras was detected. More than analogy is involved, since non-commutative integration techniques enable

one to translate the results in this measure theoretic model directly to operator theory, and to subsume thereby important aspects of operator algebra theory, this being the case, for example, with much of the Murray-von Neumann theory of approximately finite factors. Many of the stumbling blocks which beset the specialist in operator algebras, to cite non-approximately finite II_1's, are stumbling blocks in this measure theoretic model; but this model has the virtue of much greater technical simplicity, and seems the better place to confront certain unsolved problems. For the sake of unity, explicit discussion of these connections with operator theory is not undertaken in this paper. Such discussion, together with further development of the present theory itself, including non-finite measure algebras, will be given elsewhere.

2. Technical preliminaries. Any finite measure algebra is the measure algebra of a finite measure space. In turn, with each finite measure space there is associated an essentially unique measure space, having the same measure algebra, and consisting of a Stone space with a faithful normal measure. It is objects of this latter type—variously called Kakutani, perfect, or hyperstonian spaces ([1], [4])—which are studied in this work. In this selection of underlying spaces and in subsequent terminology, something of a middle course has been elected. On the one hand, many of the results carry over to general finite measure spaces; and on the other hand, the spaces actually studied are abelian W^*-algebras, as known representation theorems show. Neither fact is elaborated, the first because the really significant statements pertain to measure algebras and not to measure spaces, and the second, because use of operator terminology and methods would obscure the measure theoretic character of the study.

Let Γ be a compact hausdorff space, and let M denote the $*$-algebra $C(\Gamma)$ of complex-valued continuous function on Γ. If each bounded set f_a of real-valued functions in M has a least upper bound $f = \mathrm{LUB}\, f_a$ in M, then Γ is called a *Stone space* (see [10]). Following Dixmier [1], let Γ be a Stone space, and suppose that M admits a positive linear functional (or "measure," after Bourbaki) λ with these properties: 1) λ is *faithful*, that is, if $f \geqq 0$ and $\lambda(f) = 0$, then $f = 0$; 2) λ is *normal*, that is, for each bounded (non-void) lattice f_a of real-valued functions in M, $\lambda(\mathrm{LUB}\, f_a) = \mathrm{LUB}\, \lambda(f_a)$. [For Stone spaces, normality is equivalent to the requirement that compact sets with null interior have measure 0.] Then the space Γ is called *hyperstonian*, and the couple (Γ, λ) is called a *hyperstonian measure space*. Corrupting this usage slightly, we shall call a couple (M, λ) an *abstract hyperstonian measure space* if first, M is a commutative $(B^* = C^*)$-algebra with identity [that is,

a commutative Banach *-algebra with identity such that $\| AA^* \| = \| A \|^2$, for all A]; second, if relative to the customary order on M, positive elements being those of the form AA^*, each bounded (non-void) set of self-adjoint elements has a least upper bound; and finally, if λ is a positive faithful normal linear functional on M.

The key property of hyperstonian measure spaces is this: each bounded (Borel) measurable function f on Γ is equal almost everyhere (λ) to a continuous function ([1, Prop. 2]). In particular, the characteristic function of any measurable set is equal a. e. (λ) to a *projection*, that is, the characteristic function of a clopen set. Projections in $M = C(\Gamma)$ form a complete boolean algebra, and the measure algebra of (Γ, λ) can be identified with (M_P, λ), where M_P denotes the set of projections in M. This measure algebra (M_P, λ) completely determines (M, λ): if N is another abstract hyperstonian measure space, and if there exists a boolean isomorphism ϕ of M_P on N_P which conserves measure, then ϕ extends uniquely to a measure preserving (abbreviated, MP) isomorphism of M on N. An abstract hyperstonian measure space (M, λ) is called *non-atomic* if its measure algebra (M_P, λ) is non-atomic, that is, if each non-zero projection dominates projections of arbitrarily small positive measure.

If $(S, \mathcal{S}, m)$ is a general finite measure space, then, up to MP isomorphism, there exists precisely one abstract hyperstonian measure space (M, λ) with the same measure algebra as $(S, \mathcal{S}, m)$. One can construct this (M, λ) by taking for M the *-algebra of multiplications $L_f g = fg$ by bounded measurable functions f on $L_2(S, \mathcal{S}, m)$ under the operator norm, and for λ the linear functional $\lambda(L_f) = \int f(x)\, dm(x)$ on M. The M resulting in this construction is actually a commutative W^*-algebra of operators on a hilbert space, and λ of the construction has a representation $\lambda(A) = (Ax, x)$, for some vector x (e. g. the function 1) in that hilbert space. A theorem of Dixmier-Pallu de la Barriere asserts that any finite hyperstonian measure space has this form (up to MP isomorphisms) [1, Th. 2], so as noted above, these entities (M, λ) are in reality abelian W^*-algebras taken with faithful normal states.

Consider now an abstract non-atomic hyperstonian measure space (M, λ), with λ normalized by $\lambda(I) = 1$, fixed once and for all in the subsequent discussion of this section. A *-subalgebra N of M with identity is called hyperstonian if the couple (N, λ) is an abstract hyperstonian measure space in its own right. For this, it is sufficient that N contain, along with each bounded family A_a of self-adjoint elements, the elements $\mathrm{LUB}\, A_a$ of M.

(In fact, the validity of this condition implies that N is uniformly closed in M, and therefore B^*; the other conditions follow automatically.)

Let N be a hyperstonian subalgebra of M. Then for each A in M, there exist an element $E_N(A)$ of N such that

$$(2.1) \qquad \lambda(AB) = \lambda(E_N(A)B), \text{ for all } B \text{ in } N.$$

This follows readily from application of the Radon-Nikodym theorem and the fact that bounded measurable function are equal a.e. to continuous functions on hyperstonian spaces (in this instance, the spectrum of N). We call $E_N(A)$ the *conditional expectation of A relative to N.* Because λ is faithful, it is clear that condition (2.1) uniquely determines $E_N(A)$. The mapping E_N has the following basic properties:

(2.2) $E_N(I) = I$,

(2.3) $A \to E_N(A)$ is a *-linear positive-definite mapping,

(2.4) $E_N(AB) = E_N(A)B$, for all $A \in M$, $B \in N$,

(2.5) $\mathrm{LUB}\, E_N(A_a) = E_N(\mathrm{LUB}\, A_a)$, for each bounded lattice A_a of self-adjoint elements.

Verifications follow trivially from (2.1) and the ascribed properties of λ. Conversely, if E_N is a mapping of M into itself satisfying (2.1)-(2.5), and if $N = \mathrm{range}\, E_N$, then it follows readily that N is a hyperstonian subalgebra of M and E_N is the conditional expectation relative to N. Certain additional properties of E_N will enter. First, if α is an MP automorphism of M under which N is setwise invariant, then the relation

$$(2.6) \qquad \alpha(E_N(A)) = E_N(\alpha(A))$$

holds, this by the uniqueness of mappings E_N satisfying (2.1). Second, use of the inequality $\lambda[(A - E_N(A))(A - E_N(A))^*] \geqq 0$ establishes

$$(2.7) \qquad \lambda(E_N(A)E_N(A^*)) \leqq \lambda(AA^*).$$

Finally, defining the *N-carrier* of an element A in M to be the greatest lower bound of projections P in N satisfying $PA = A$, one observes that, if $A \geqq 0$, then A and $E_N(A)$ have the same N-carrier.

A notion of type, related to the dimension type concept of operator theory, is introduced as follows. Let N be a hyperstonian subalgebra of M. A non-zero projection P in M is called *abelian* over N if each projection Q in M, $Q \leqq P$, has the form $Q = PC$, for some C in N_P. [One has, equivalently,

$Q \leqq P$ entails $E_N(Q) = CE_N(P)$, for some C in N.] We say that N is a *type I subalgebra* of M if each non-zero projection in M dominates a projection abelian over N. On the other hand, if M contains no projections abelian over N, we say that N is a *type II subalgebra* of M.

Let G be a group of MP automorphisms $A \to gA$ of M. [Throughout, by convention, automorphism $=$ *-automorphism.] By the *fixed algebra* of G we mean the algebra $Z = [A \in M \mid gA = A$, for all $g \in G]$. Necessarily, Z is hyperstonian, and the preceding concepts of type apply. G is called type I (respectively, type II) group if Z is a type I (respectively, type II) subalgebra of M. Mixed types can occur, of course, but a natural device enables one to split G into purely type I and type II parts. Expressly, since the translate by any member of G of a type I projection over Z is again a type I projection over Z, it follows that the Z-carrier of a type I projection is again a type I projection over Z. In turn, the least upper bound C of all type I projection will be a type I projection which lies in Z, and the projection $I - C$ will be of type II. Now CM and $(I-C)M$ are hyperstonian algebras (with identities C and $I - C$) of types I and II, each reduces G, and M is the direct sum of CM and $(I-C)M$. When G is full (Section 3), G splits into the direct sum $G_C + G_{(I-C)}$ of two groups, the first a type I group of MP automorphisms of CM, the second a type II group MP automorphisms of $(I-C)M$. The summands are obviously uniquely determined. Thus the study of MP automorphism groups reduces to the study of groups which are either of type I or of type II.

A useful technical device for the type II theory can be adapted from a lemma of Maharam [6], used in her classification of homogeneous measure algebras.

MAHARAM'S LEMMA. *Assume that N is a type II subalgebra of M. Then under the expectation mapping E_N, the set of projections Q in M, which are dominated by some fixed P in M_P, maps onto the set of A in N with $0 \leqq A \leqq E_N(P)$.*

This is proved by an argument identical with Maharam's; the present condition, that P dominates no abelian projections, functions in the same way in proof as Maharam's condition that the cardinality of the principal ideal PM_P exceed that of PN_P, for each non-zero P. For the sake of completeness, we give a brief sketch of details. First one notes that, by normality of E_N, it suffices to show that, given $A \neq 0$ in N with $0 \leqq A \leqq E_N(P)$, there exists a non-zero projection $Q \leqq P$ such that $E_N(Q) \leqq A$. Now one makes a

further reduction. Let C be a projection in N with the property that $E_N(P)$ is positive on the clopen subset of the spectrum Γ_N of N corresponding to C, and let n be a positive integer. For proof, it suffices to show that a projection $Q \leqq P$ exists such that $0 < E_N(Q) \leqq E_N(P)/2^n$ on C. One arrives at such a Q as follows. The key step is to observe that, because P dominates no abelian projections, a projection R will exist such that $0 < E_N(R) < E_N(P)$ on C. Choosing such an R, let D_1 (respectively, D_2) be the projection in N corresponding to the sets

$$[\gamma \text{ in } \Gamma_N \mid 2E_N(R)(\gamma) \geqq E_N(R)(\gamma)], \qquad [\gamma \text{ in } \Gamma_N \mid 2E_N(R)(\gamma) \leqq E_N(P)(\gamma)];$$

the projection $Q_1 = D_1(P - R) + D_2 R$ then satisfies $0 < E_N(Q_1) \leqq E_N(P)/2$ on C. Continuing this construction, with Q_1 replacing P, etc., one arrives at the desired Q, and the lemma follows.

Finally, we review certain action characteristics of measure preserving automorphisms. Let α be an MP automorphism of M. A projection P in M is said to be *absolutely fixed* under α if $\alpha(Q) = Q$, for each $Q \leqq P$. Plainly, ere exists a maximal projection F_α absolutely fixed under α. We say that α is *freely-acting* if $F_\alpha = 0$. In turn, a group G of MP automorphisms of M is called freely-acting if $F_g = 0$, for each $g \neq e$ (the identity) in G. [It should be stressed that certain applications require a definition of free action which, for non-countable groups, is more stringent: specifically, under the latter definition, G is called freely acting if the set of points in the spectrum of M, each fixed under the induced action of some element $\neq e$ of G, is a set of measure zero.] This concept of free action (due to von Neumann) can be viewed as a natural relaxation of the notion of ergodicity, where by definition an automorphism is ergodic if it leaves no non-trivial projections fixed. Any ergodic automorphism is of course freely acting. However, the powers of α^n of an ergodic automorphism α need not be ergodic, whereas they are automatically freely acting in our non-atomic case. [If $\alpha^n(P) = P$, with α ergodic, then application of the ergodic theorem shows that $\lambda(P) = r/n$, for some integer $0 \leqq r \leqq n$, so plainly, α^n cannot leave arbitrarily small projections fixed.] As is customary, a group G of MP automorphisms is called *ergodic* if no non-trivial projections are simultaneously fixed under all members of G.

The construction of examples in this theory frequently involves representation of abstract groups as freely-acting automorphism groups. To assure existence of such representations, we append the following lemma.

LEMMA 2.1. *Any infinite discrete group can be faithfully represented*

as an ergodic group of freely-acting MP automorphisms of a non-atomic measure algebra.

Proof. Let S be a torsion-free discrete abelian group, and let α be an automorphism of S. The character group $\hat{S}$ of S is a connected compact abelian group, and α induces an automorphism $\hat{\alpha}$ of $\hat{S}$ defined by the relation $(\hat{\alpha}\hat{s}, s) = (\hat{s}, \alpha s)$, where $s \in S$ (respectively, $\hat{s} \in \hat{S}$) and $(\hat{s}, s)$ denotes the value of s in the character $\hat{s}$. Automatically, $\hat{\alpha}$ is haar measure preserving. In addition, we claim, $\hat{\alpha}$ is either freely-acting or trivial. Suppose there exists a measurable set E_1 in $\hat{S}$ with positive measure which is absolutely fixed under $\hat{\alpha}$, that is, for each measurable subset F of E_1, F and $\hat{\alpha}F$ differ by a set of measure 0. It follows easily that some measurable subset E of E_1 with positive measure will be pointwise fixed under $\hat{\alpha}$. In turn, $E^{-1}E$ is pointwise fixed. Because $E^{-1}E$ contains a neighborhood of the identity and $\hat{S}$ is connected, it follows that $\hat{\alpha}$ is the identity.

Applying this, let G be an infinite discrete group, and let S be the additive abelian group of integer-valued functions on G with compact support. Each g in G implements an automorphism $(\alpha_g s)(h) = s(gh)$ of this torsion-free group S, and it is clear that $g \to \hat{\alpha}_g$ is a faithful representation of G as a group of MP automorphisms of $\hat{S}$ under haar measure. The first paragraph shows that this action of G on $\hat{S}$ is free. We observe, finally, that these $\hat{\alpha}_g$ form an ergodic group. In fact, if a bounded measurable function $f \neq 0$ on $\hat{S}$ is invariant under all $\hat{\alpha}_g$, then the fourier transform $\hat{f}$ of f, as a function on S, will be constant on each orbit of G in S. Because f is square-integrable, and the orbit of each $s \neq 0$ in S under G is infinite, it follows that $\hat{f}$ must vanish except at 0, and therefore, that f is constant a. e. This proves the lemma, since the $\hat{\alpha}_g$ in particular determine automorphisms of the measure algebra of $\hat{S}$.

3. Full groups of measure preserving automorphisms. Throughout this section, (M, λ) will denote a fixed non-atomic abstract hyperstonian measure space.

Definition 3.1. Given two automorphisms α and β of M, denote by $F(\alpha, \beta)$ the maximal projection in M absolutely fixed under $\alpha^{-1}\beta$. [Clearly, $F(\alpha, \beta) = F(\beta, \alpha)$.] If G is any group of MP automorphisms of M, and if α is any automorphism of M, we say that α depends on G if $\mathrm{LUB}_{g \in G} F(\alpha, g) = I$ (the identity projection). Denote by $[G]$ the collection of all automorphisms of M which depend on G. $[G]$ is called the *full group* determined by G,

and a group G is called full if $G=[G]$. Two groups G_1 and G_2 of MP automorphisms of M are *equivalent* if they determine the same full group, that is, if $[G_1]=[G_2]$.

The condition that an automorphism α of M depend on a group G can be phrased in terms of the spectrum Γ of M: expressly, α lies in $[G]$ if and only if there exists a set Γ_0 in Γ having measure 0 and such that, for each γ in $\Gamma-\Gamma_0$, a clopen set P containing γ and a g in G exist such that the homeomorphisms of Γ induced by α and g agree at all points of P. (The exceptional set Γ_0 will be closed and nowhere dense.) The conventional notion of equivalence of groups G_1 and G_2 requires the existence of an MP automorphism φ of M such that $\varphi^{-1}G_1\varphi=G_2$. In particular, this implies that G_1 and G_2 are isomorphic as groups. Nothing of this sort is true for the present notion of equivalence, however. The one obvious necessary condition for equivalence, as the following lemma shows, is that G_1 and G_2 have the same fixed algebra; after this, particularly in the type *II* case, it becomes a highly technical problem to obtain revealing criteria for equivalence. This difficulty does not affect the theory, however, because full groups are the natural objects to study, and significant statements are invariant under equivalence.

LEMMA 3.1. *For any group of MP automorphisms of M, $[G]$ is again a group of MP automorphisms of M, and $[\![G]\!]=[G]$. If G_1 is any subgroup of $[G]$, then the fixed algebra of G_1 contains that of G. Finally, elements α of $[G]$ are precisely those endomorphisms of M having a representation*

$$\alpha(P)=\sum_n P_n\beta_n(P), \tag{3.1}$$

where the $\beta_n\in G$, and P_n (resp. $\beta_n^{-1}(P_n)$) is a mutually orthogonal set of projections in M having least upper bound I.

Proof. First, any α in $[G]$ is automatically measure preserving. In fact, this follows because each $P\neq 0$ dominates a $Q\neq 0$ on which α is MP.

Next, we assert, α in $[\![G]\!]$ entails α in $[G]$. For this, it will suffice to show that, given $P\neq 0$, there exists a $g\in G$ such that $F(\alpha,g)P\neq 0$. Choose β in $[G]$ such that $F(\alpha,\beta)P\neq 0$. Because $\mathrm{LUB}_g F(\beta,g)P=P$, we can choose $g\in G$ so that $F(\alpha,\beta)F(\beta,g)P\neq 0$. But $F(\alpha,\beta)F(\beta,g)\leqq F(\alpha,g)$, hence $F(\alpha,g)P\neq 0$.

To show that $[G]$ is a group, it suffices to prove that, given α and β in $[G]$ and $P\neq 0$, there exists an element $k\in G$ such that $F(\alpha^{-1}\beta,k)P\neq 0$. To do this, choose g in G such that $F(\beta,g)P\neq 0$. Because $\mathrm{LUB}_h\,\beta^{-1}\alpha(F(\alpha,h))$

$=I$, we can choose $h \in G$ to satisfy $\beta^{-1}\alpha[F(\alpha,h)]F(\beta,g)P \neq 0$. Consider any Q dominated by the latter projection. Since $\alpha^{-1}\beta Q \leqq F(\alpha,h)$, we have $h\alpha^{-1}\beta(Q) = \alpha(\alpha^{-1}\beta(Q)) = \beta(Q) = gQ$, so $\alpha^{-1}\beta Q = h^{-1}gQ$. Setting $k = h^{-1}g$, we have $F(\alpha^{-1}\beta, k)P \neq 0$, as desired.

If α lies in $[G]$, and if $gP = P$, for all g in G, then

$$\alpha P = \mathrm{LUB}_g\, \alpha[F(\alpha,g)P] = \mathrm{LUB}_g\, g[F(\alpha,g)P] = P.$$

In particular, therefore, P lies in the fixed algebra of any subgroup G_1 of $[G]$.

Fix an α in $[G]$. To show that α has a representation (3.1), we apply Zorn's lemma to construct a maximal set of mutually orthogonal non-zero projections P_a, subject to the requirement that each P_a be dominated by a projection $\alpha F(\alpha,\beta)$, for some β in G depending on P_a. Of necessity, P_a is countable set, and we write $P_n \leqq \alpha F(\alpha,\beta_n)$. The projection $P = I - \sum_n P_n$ must be 0; otherwise, because $\mathrm{LUB}_\beta\, \alpha F(\alpha,\beta) = I$, there will exist a non-zero projection of the form $P\alpha F(\alpha,\beta)$, contradicting maximality. Now $\alpha^{-1}P_n \leqq F(\alpha,\beta_n)$, hence $\alpha(\alpha^{-1}P_n) = \beta_n(\alpha^{-1}P_n)$, and $\beta_n^{-1}P_n = \alpha^{-1}P_n$. Therefore, $\sum \beta_n{}^{1}P_n = \sum \alpha^{-1}P_n = I$, $\sum$ denoting LUB. Finally, $\alpha(P) = \sum P_n\alpha(P) = \sum \alpha(P\alpha^{-1}P_n) = \sum \beta_n(P\beta_n^{-1}P_n) = \sum P_n\beta_n P$, proving (3.1). Conversely, if P_n (resp. $\beta_n^{-1}P_n$) is a set of mutually orthogonal projections with LUB I, and if we set $\alpha(P) = \sum P_n\beta_n P$, $\beta(P) = \sum \beta_n^{-1}(P_nP)$, then direct computation shows that both α and β are boolean endomorphisms of M_P and that $\alpha\beta P = \beta\alpha P = P$, for all P. [To justify this computation, one should bear in the relations $\mathrm{LUB}_{a,b}\, P_bQ_a = (\mathrm{LUB}\, P_a)(\mathrm{LUB}\, Q_b)$ and $\mathrm{LUB}\, P_a \cup \mathrm{LUB}\, Q_b = \mathrm{LUB}\, P_a \cup Q_a$, which hold for arbitrary sets P_a, Q_b in M_P, a and b describing a common index set.] Therefore, α and β are boolean isomorphisms of M_P and $\beta = \alpha^{-1}$. Both conserve measure: e.g.

$$\lambda(\alpha P) = \sum \lambda(P_n\beta_n P) = \sum \lambda(\beta_n^{-1}(P_n)P) = \lambda(P).$$

This completes the proof.

Consider a group G of MP automorphisms of M, with fixed algebra denoted Z. If $\alpha \in [G]$, and if $\alpha P \leqq Q$, for certain projections P and Q in M, then properties (2.3) and (2.6) of the mapping E_Z give $E_Z(Q) \geqq E_Z(\alpha P) = \alpha E_Z(P) = E_Z(P)$. A key fact is, the converse holds.

LEMMA 3.2. *Let G be a group of MP automorphisms of M with fixed algebra Z. If $E_Z(P) \leqq E_Z(Q)$, for projections P and Q in M, then there exists an α in $[G]$ with these properties: $\alpha P \leqq Q$; α^2 is the identity; and α is the identity off $P \cup \alpha P$.*

Proof. Assume, to begin, that $PQ=0$. We have noted earlier that the Z-carrier $\bar{P}=\mathrm{LUB}_{\beta\in[G]}\beta P$ of P coincides with the Z-carrier (that is, the support) of $E_Z(P)$. Therefore, $E_Z(P)\leqq E_Z(Q)$ forces $\bar{P}\leqq\bar{Q}$. It follows that $[G]$ contains an α_1 such that $\alpha_1(P)Q\neq 0$. If we set $Q_1=\alpha_1(P)Q$, $P_1=\alpha_1^{-1}(Q_1)$, then (P_1,Q_1,α_1) is a triple with these properties: $\alpha_1\in[G]$, $0\neq P_1\leqq P$, and $Q_1=\alpha_1(P_1)\leqq Q$. By Zorn, we may construct a maximal set (P_a,Q_a,α_a) of triples satisfying these conditions, and subject to the further requirement that the P_a (respectively the Q_a) be a mutually orthogonal set. This maximal set will contain only countably many members (P_n,Q_n,α_n), and further, by the normality of E_Z, we have $E_Z(P-\sum P_n)\leqq E_Z(Q-\sum Q_n)$. Maximality forces $P=\sum P_n$: otherwise, the above argument applied to $P-\sum P_n$ and $Q-\sum Q_n$ would yield a new triple orthogonal to all the (P_n,Q_n,α_n). Let $\alpha=\alpha_n$ on P_n, α_n^{-1} on Q_n, and the identity off $P\cup\alpha P$. By construction and (3.1), α satisfies the conditions of the lemma. The general case, in which no restriction is made on PQ, follows directly if we apply the above case to $P-PQ$ and $Q-PQ$.

The following specialization of Lemma 3.2 is useful.

LEMMA 3.3. *Let G be a group of MP-automorphisms of M, with fixed algebra Z, and let $P_0,P_1,\cdots,P_{n-1}$ be mutually orthogonal projections in M with $E_Z(P_0)=E_Z(P_1)=\cdots=E_Z(P_{n-1})$. Then $[G]$ contains an α with these properties: $\alpha P_i=P_{i+1}$ (indices* mod n), *α^n is the identity, and α is the identity off $P_0+\cdots+P_{n-1}$.*

Proof. For each $i>0$ choose β_i in $[G]$ such that $\beta_i(P_0)=P_i$, β_i^2 is the identity, and β_i is the identity off P_0+P_i. Put $\alpha=\beta_{n-1}\cdots\beta_1$. Then if $Q\leqq P_i$, $\alpha Q=\beta_{i+1}\beta_iQ\leqq P_{i+1}$, $\alpha^2Q=\beta_{i+2}\beta_iQ$, etc., until $\alpha^nQ=\beta_{i+n}\beta_iQ=\beta_i^2Q=Q$.

LEMMA 3.4. *Let α be an arbitrary MP automorphism of M, and G a given group of MP automorphisms. Then there evists a unique maximal projection $E([G],\alpha)$ and a β in $[G]$ with the property that, for all Q in M, $E([G],\alpha)\alpha(Q)=E([G],\alpha)\beta(Q)$. One has*

$$E([G],\alpha)=\mathrm{LUB}_{\gamma\in[G]}\alpha F(\alpha,\gamma)=\alpha F(\alpha,\beta). \tag{3.2}$$

Proof. If no pair $P\neq 0$, $\beta\in[G]$ exists such that $P\alpha Q=P\beta Q$, for all Q, set $E([G],\alpha)=0$. In the contrary case, denote by P_a, β_a the collection of all such pairs, and set $P=\mathrm{LUB}\,P_a$. Clearly, we can choose from P_a, β_a a subsequence P_n, β_n such that the P_n are mutually orthogonal and $P=\sum P_n$. By construction, $P_n\alpha Q=P_n\beta_nQ$, for all Q and n, whence

$$\alpha^{-1}(P_n)Q=\alpha^{-1}(P_n)\alpha^{-1}\beta_n(Q),$$

and substitution of $Q=\beta_n^{-1}(P_n)$ here gives $\alpha^{-1}(P_n)\leqq\beta_n^{-1}(P_n)$. This inequality reverses by symmetry, yielding $\alpha^{-1}(P_n)=\beta_n^{-1}(P_n)$. Using this, we have $E_Z(\alpha^{-1}P)=\sum E_Z(\alpha^{-1}P_n)=\sum E_Z(\beta_n^{-1}P_n)=\sum E_Z(P_n)=E_Z(P)$, where Z denotes the fixed algebra of G. Therefore, by Lemma 3.2, there exists a β_0 in $[G]$ such that $\beta_0(I-P)=\alpha^{-1}(I-P)$, $\beta_0^2=$ identity, $\beta_0=$ identity off $(I-P)\cup\alpha^{-1}(I-P)$. Setting $P_0=I-P$, we observe that P_n (resp. $\beta_n^{-1}P_n$) is for $n\geqq 0$ a mutually orthogonal set with LUB I. Applying Lemma 3.1, it follows that $\beta^{-1}(Q)=\sum_{n=0}^{\infty}\beta_n^{-1}(P_nQ)$ defines an element β of $[G]$. Now

$$P\beta Q=\beta(Q\beta^{-1}P)=\beta[\sum_{n-1}^{\infty}\beta_n^{-1}(P_n)Q]$$

$$=\beta[\sum_{n-1}^{\infty}\beta_n^{-1}(P_n\beta_n(Q))]=\beta[\sum_{n=1}^{\infty}\beta_n^{-1}(P_n\alpha Q)]=\beta[\beta^{-1}(P\alpha Q)]=P\alpha Q.$$

This projection $P=E([G],\alpha)$ has the ascribed properties, maximality following by construction. Turning to (3.2), one has, first, $\mathrm{LUB}_{\gamma\in[G]}\alpha F(\alpha,\gamma)\leqq P$; in fact, if γ in $[G]$ and $R\neq 0$ satisfy $R\leqq\alpha F(\alpha,\gamma)$ and $PR=0$, then R,γ is a pair with R orthogonal to all P_a, a contradiction. Next, $P\leqq\alpha F(\alpha,\beta)$: if $Q\leqq\alpha^{-1}P$, then $Q=(\alpha^{-1}P)Q=\alpha^{-1}P\alpha^{-1}\beta Q\leqq\alpha^{-1}\beta Q$, forcing $\alpha Q=\beta Q$, and $\alpha^{-1}P\leqq F(\alpha,\beta)$. The final link, $\alpha F(\alpha,\beta)\leqq\mathrm{LUB}_{\gamma\in[G]}\alpha F(\alpha,\gamma)$, is obvious.

Given a group G of MP automorphisms of M with fixed algebra Z, and a non-zero projection P in M, we introduce the local group (discussed in Section 1) by setting $[G]_P=[\alpha$ in $[G]\,|\,\alpha$ leaves $I-P$ absolutely fixed$]$.

LEMMA 3.5. *If Z' denotes the fixed algebra of $[G]_P$, then $Z'P=ZP$. In particular, if G is of type II, then so is the summand $[G]_PP$ of $[G]_P$.*

Proof. The inclusion $ZP\subset Z'P$ is clear. To prove equality, we proceed by indirect proof, assuming $ZP\subset Z'P$ properly. There will exist, then, an $R\leqq P$, R in Z', such that the Z-carriers of $P-R$ and R overlap, whence $\alpha(R)(P-R)\neq 0$, for some α in $[G]$. In particular, for some non-zero $R_1\leqq R$, $\alpha(R_1)=R_2\leqq P-R$. Set $\beta=\alpha$ on R_1, α^{-1} on R_2, identity elsewhere. Then β lies in $[G]_P$ and $\beta(R_1)=R_2$. Because β must leave R fixed, we have $R_2\beta R_1\leqq(P-R)\beta R=(P-R)R=0$, which is absurd, so the first statement of the lemma is proved. Now if $[G]_PP$ is not of type II, then there exists a projection $Q\leqq P$ abelian over Z'. But $Z'P=ZP$, so Q is abelian over Z, and G cannot be of type II. This proves the lemma.

PROPOSITION 3.1. *Let G be a full type II group of MP automorphisms of M, and let Z be the fixed algebra of G. Then* 1) *any G-invariant*

intermediate hyperstonian subalgebra N, $M \supset N \supset Z$, *has the form* $N = ZC + M(I - C)$, *for some* C *in* Z_P, *and* 2) *any full normal subgroup* K *of* G *has the form* $K = G_C$, *for some* C *in* Z_P.

Proof. Let C be the maximal projection in Z with the property $CZ = CN$. By dropping down to the summand $G_{(I-C)}$ on $(I - C)M$, we may assume $C = 0$. This done, we claim first that the N of assertion (1) is of type II over Z. Suppose to the contrary that a projection P in N is abelian over Z (relative to N). Because $C = 0$, P does not lie in Z, and we have

$$A = E_Z(P) \wedge E_Z(I - P) \neq 0.$$

Therefore, by Maharam's lemma, there exist projections P_0, P_1, P_2 in M with the following properties: P_0 and P_1 are dominated by P, $P_2 \leqq I - P$; the P_i are mutually orthogonal; and $E_Z(P_i) = A/2$, for each i. Applying Lemma 3.3, choose an α in G such that $\alpha(P_i) = P_{i+1}$ (indices mod 3), $\alpha^3 = \text{identity}$, $\alpha = \text{identity}$ off $P_0 + P_1 + P_2$. Because N is G-invariant, the projection $P\alpha P$ lies in N, and further, because P is assumed abelian, $P\alpha P = PE$, for some E in Z. Now

$$\begin{aligned} P - P_0 = P\alpha P = PE = P\alpha(P\alpha P) &= P\alpha(P - P_0) \\ &= P\alpha P - P_1 = P - P_0 - P_1. \end{aligned}$$

This forces $P_1 = 0$, a contradiction, and it follows that N is of type II over Z. This being the case, let Q be any projection in M, and apply Maharam's lemma to conclude that $E_Z(P) = E_Z(Q)$, for some P in N. By Lemma 3.2, $\beta P = Q$, for some β in G. Therefore, $Q \in N$, by the G-invariance of N, and we have proved $N = M$.

Now let K be a full normal subgroup of G. Let C be the maximal projection in M left absolutely fixed by all β in K. For any α in G and any $Q \leqq \alpha C$, $\alpha\beta\alpha^{-1}Q = Q$, and $\alpha\beta\alpha^{-1} \in K$. Thus αC is also absolutely fixed under K, for all α in G. By maximality, therefore, $C \in Z$. As above, dropping to $G_{(I-C)}$ on $(I - C)M$ if necessary, we assume $C = 0$. This done, let Z_0 be the fixed algebra of K. Because K is normal, Z_0 is a G-invariant intermediate hyperstonian subalgebra of M, and so the first paragraph of proof together with the assumption $C = 0$ entail $Z_0 = Z$. By Maharam's lemma, choose a projection P such that $E_Z(P) = E_Z(I - P)$. By Lemma 3.2 applied to K, there exists a β in K such that $\beta P = I - P$, $\beta^2 = \text{identity}$. Take any α in G_P. Then $\beta\alpha^{-1}\beta\alpha \in K$, and for $Q \leqq P$, $\beta\alpha^{-1}\beta\alpha Q = \beta^2\alpha Q = \alpha Q$. This proves that $K_P = G_P$. Likewise, $K_{(I-P)} = G_{(I-P)}$. Consider an arbitrary α in G. We

have $E_Z(P) = E_Z(\alpha P)$, so there exists a γ in K such that $\gamma^{-1}\alpha P = P$. Clearly, then, $\gamma^{-1}\alpha$ is the product of an element in $G_P = K_P$ and an element in $G_{(I-P)} = K_{(I-P)}$. This implies $\gamma^{-1}\alpha \in K$, so in turn, $\alpha \in K$. Therefore, $K = G$, and the proof is completed.

Proposition 3.1 holds without restriction to type II groups; the proof for the type I case follows easily out of results in the next section.

4. Groups of Type *I*. The structure of type I groups, as we shall see in this section, can be described rather completely: any type I group is "almost" equivalent to a finite group. Their technical interest lies in their very simplicity, in that one is led to see how much information can be gleaned about an arbitrary full group by study of its type I subgroups alone. Again, in this section, (M, λ) will denote an abstract non-atomic hyperstonian measure space.

Lemma 4.1. *Let G be a group of MP automorphisms of M, let Z be the fixed algebra of G, and let Q be a projection abelian over Z. Then* 1) *if α and $\beta \in [G]$, and if for some projection P, $\alpha(P) \leqq Q$ and $\beta(P) \leqq Q$, then $\alpha(P) = \beta(P)$*; 2) *if $\alpha \in [G]$ is freely acting, then $\alpha(Q)Q = 0$*; 3) *if P is another projection abelian over Z with the same Z-carrier as Q, then $E_Z(P) = E_Z(Q)$.*

Proof. Re (1) Choose C and D in Z_P so that $\alpha(P) = PC$ and $\beta(P) = PD$. Then $\alpha(P - PC) = \alpha(P)(I - C) = 0$, so that $P = PC$. Likewise, $P = PD$. Therefore, $\alpha(P) = \alpha(PD) = QCD = \beta(PC) = \beta(P)$. Re (2) If $Q\alpha Q \neq 0$, then a non-zero $R \leqq Q$ exists such that $\alpha(R) \leqq Q$. Applying (1) with $\beta =$ identity, and P arbitrary $\leqq R$, it follows that $\alpha(P) = P$. Therefore, R is absolutely fixed under α, a contradiction. Re (3) Assume to the contrary that $E_Z(P) \neq E_Z(Q)$. We can assume that a $C \in Z_P$ exists such that $E_Z(QC) - E_Z(PC) \geqq 0$, but not $= 0$. By Lemma 3.2, an α in $[G]$ exists such that $\alpha(PC) \leqq QC$, $E_Z(QC - \alpha(PC)) \neq 0$. Hence there exists an $R \leqq QC$ such that $R\alpha(PC) = 0$. Denoting by $\bar{P}$ the Z-carrier of P, we have $R \leqq \bar{P}C$, so there exists a non-zero projection $S \leqq \bar{P}C$ and a $\beta \in [G]$ such that $\beta(S) \leqq R$. Now $\alpha(S) \leqq Q$, $\beta(S) \leqq Q$, and $\alpha(S)\beta(S) = 0$. This contradicts (1).

A corollary here is noteworthy. If G is infinite and freely acting, then (2) shows that no abelian projections can exist over the fixed algebra Z of G: were Q abelian over Z, then we would have $QgQ = 0$, for each g in G, $g \neq e$, and in turn, $gQhQ = 0$, for each pair $g \neq h$ in G; the set gQ is then infinite

and mutually orthogonal, contradicting the finiteness of λ. Therefore, *any freely acting infinite group is of type II.*

LEMMA 4.2. *Two type I MP groups G_1 and G_2 are equivalent if and only if they have the same fixed algebra.*

Proof. Necessity follows from Lemma 3.1. For sufficiency, denote by Z the common fixed algebra of G_1 and G_2, and consider some fixed α in $[G_1]$. If Q is any projection abelian over Z, and if β in $[G_2]$ is chosen so that $\beta(Q)=\alpha(Q)$, this being possible by Lemma 3.2, since $E_Z(Q)=E_Z(\alpha Q)$, then $Q\leqq F(\alpha,\beta)$; for any $P\leqq Q$ has the form $P=QC$ $(C\in Z)$, and hence $\alpha(P)=\alpha(Q)C=\beta(P)$. The identity I being the least upper bound of projections abelian over Z, it follows that $\mathrm{LUB}_{\beta\in[G_2]}F(\alpha,\beta)=I$, so $\alpha\in[G_2]$. Therefore, $[G_1]\subset[G_2]$, and equality follows by symmetry.

Definition 4.1. Let G be a group of MP automorphisms of M with fixed algebra Z. The group G is said to be of type I_n $(n=1,2,\cdots)$ if there exist mutually orthogonal projections $P_1,\cdots,P_n$ in M, each abelian over Z, such that $\sum_i P_i=I$ and $E_Z(P_1)=\cdots=E_Z(P_n)$. Such a set $P_1,\cdots,P_n$ is called an *abelian basis* for G.

LEMMA 4.3. (1) *Each type I group can be decomposed in one and only one way as a direct sum of type I_n groups $(n=1,2,\cdots)$*; (2) *Any group of type I_n is equivalent to a freely-acting cyclic group of order n, and any freely-acting group of order n is of type I_n*; (3) *A freely acting group G of order n has an abelian basis of the form $[gP \mid g\in G]$, and conversely, if P is any projection in M such that the gP are mutually orthogonal and have* LUB I, *then the gP form an abelian base for G.*

Proof. (1) We claim, first, that the identity I can be partitioned $I=\sum P_n$ as a sum of mutually orthogonal abelian projections in such a way that the Z-carriers C_i of P_i form a decreasing sequence; and that if $I=\sum P'_n$ is another partition of I with the same properties, then the Z-carrier of $P'_i=C_i$, for all i.

By definition, any non-zero projection Q dominates a projection P abelian over Z. This P can be chosen so that Z-carrier $P=Z$-carrier Q, as follows readily from the fact that, if R_n is a sequence of abelian projections with mutually orthogonal Z-carriers, then $\sum R_n$ is likewise abelian. To prove existence of the partition described above, let P_1 be an abelian projection with Z-carrier $C_1=I$, and inductively, let P_n be an abelian projection

$\leqq I - \sum_{i<n} P_i$ with Z-carrier $C_n = Z$-carrier of $I - \sum_{i<n} P_i$. Plainly, $C_1 \geqq \cdots \geqq C_n \geqq \cdots$. Let C be the Z-carrier of $I - \sum P_n$. Then for all n, $C \leqq Z$-carrier $(I - \sum_{i<n} P_i) = C_n$, so the projections CP_n all have the same Z-carrier C. If $C \neq 0$, then (3) in Lemma 4.1 shows that $E_Z(P_1C) = E_Z(P_nC)$ for all n, whence $\lambda(I) \geqq \lambda[E_Z(P_1C + \cdots + P_nC)] = n\lambda(P_1C)$ for all n, contradicting the finiteness of λ. Let $I = \sum P'_i$ be another dissection of I into mutually orthogonal abelian projections with decreasing Z-carriers C'_i. Plainly $C'_1 = I = C_1$, and granting $C'_i = C_i$, for $i < n$, another application of (3) in Lemma 4.1 gives $E_Z(I - \sum_{i<n} P_i) = E_Z(I - \sum_{i<n} P'_i)$, and therefore,

$$C'_n = Z\text{-carrier}(\sum_{i\geqq n} P'_i) = Z\text{-carrier } (I - \sum_{i<n} P'_i) = Z\text{-carrier } (I - \sum_{i<n} P'_i)$$
$$= Z\text{-carrier } E_Z(I - \sum_{i<n} P_i) = Z\text{-carrier } (I - \sum_{i<n} P_i) = C_n.$$

This proves the assertion of the first paragraph.

Define $D_n = C_n - C_{n+1}$ $(n \geqq 1)$. Now $\sum_{k\leqq n} D_k = I - C_n$, and since either $C_n = 0$ for some n, or $C_n \neq 0$ for all n but $\mathrm{GLB}\, C_n = 0$, as the above argument shows, we must have $\sum D_n = I$. Further, $D_n = D_nP_1 + \cdots + D_nP_n$, the projections D_nP_i are abelian with Z-carrier D_n, and therefore, $E_Z(D_nP_1) = \cdots = E_Z(D_nP_n)$. It follows that $[G] = \sum [G]_{D_n} D_n$, and $[G]_{D_n}$ on D_nM is by definition of type I_n. Let D'_n be another sequence of mutually orthogonal projections in Z such that $\sum D'_n = I$, and $D'_n = R_1^{(n)} + \cdots + R_n^{(n)}$, with $R_i^{(n)}$ abelian and $E_Z(R_1^{(n)}) = \cdots = E_Z(R_n^{(n)})$. We will show that $D'_n = D_n$, for all n. In fact, let $P'_n = \sum_{k, k\geqq n} R_n^{(k)}$. The P'_i are abelian and $\sum P'_n = I$. Further, Z-carrier $P'_n = C'_n = \mathrm{LUB}_{k, k\geqq n}\, Z\text{-carrier } R_n^{(k)} = \sum_{k\geqq n} D'_k$. The C'_n consequently decrease with n, and the uniqueness assertion of the first paragraph implies $C'_n = C_n$, for all n. Hence, $D_n = C_n - C_{n+1} = C'_n - C'_{n+1} = D'_n$, and (1) is established.

(2) and (3). Let K be a group of type I_n, with fixed algebra denoted Z. Let $P_0, \cdots, P_{n-1}$ be an abelian base for K over Z. Because the P_i have the same expectation relative to Z, we can apply Lemma 3.3 to select an α in $[K]$ such that $\alpha P_i = P_{i+1}$ (indices mod n) and $\alpha^n =$ identity. Trivially, the group G generated by α is freely acting of order n, and by construction, $[G] \subset [K]$. To prove that $[G] = [K]$, it suffices by Lemma 4.2 to show that each P in the fixed algebra of $[G]$ already lies in Z. For this, let C be the projection in Z such that $PP_0 = CP_0$, and compute

$$P - C = (P - C)(\sum_{i=0}^{n-1} \alpha^i P_0) = (\sum_{i=0}^{n-1} \alpha^i[(P - C)P_0] = 0.$$

Let G be a freely acting group of order n. If g is any element of G not e, then by free action, given any non-zero projection Q, there exists a non-zero $R \leqq Q$ such that $RgR = 0$. Enumerate the elements of G not e as $g_1, \cdots, g_{n-1}$, let R_1 be a non-zero projection such that $R_1 g_1 R_1 = 0$, let R_2 be a non-zero projection $\leqq R_1$ such that $R_2 g_2 R_2 = 0$, etc. We arrive at a non-zero projection P $(= R_{n-1})$ such that $PgP = 0$, for all $g \neq e$. If $g \neq h$, then $gPhP = g[Pg^{-1}hP] = 0$. By Zorn, we can assume that no larger projection $P_1 \geqq P$ has this property $P_1 g P_1 = 0$ (all $g \neq e$). But then $\sum gP = I$: for $C = \sum gP$ lies in the fixed algebra Z of G, and were $I - C \neq 0$, we could apply the above argument to $I - C$ to obtain a projection P' orthogonalized by G and $\leqq I - C$; the projection $P' + P$ is then orthogonalized by G and is larger than P, a contradiction. The projection P is abelian over Z, since each $R \leqq P$ has the form $R = (\sum gR)P$ and $\sum gR \in Z$. Consequently, all the projections gP are abelian over Z, and therefore, G has an abelian base of the form prescribed in (3). This base has n elements, and therefore G is a type I_n. The lemma follows.

Let G be a type I group with fixed algebra Z. We will call R a *bounded* (type I) group if the identity is a finite union of projections abelian over Z. This means that G has only finitely many "pure," or type I_n, constituents, and a simple application of Lemma 4.3 (2) shows in fact that G is equivalent to a finite group. Conversely, it is evident that any group equivalent to a finite group must be a bounded type I. A related observation, useful in later work, is the following:

LEMMA 4.4. *Let F be a finite set of MP automorphisms of M which leave fixed (pointwise) a bounded type I subalgebra of M. Then the group G_F of MP automorphisms generated by F is of finite order.*

Proof. By hypothesis, $[G_F]$ is a finite direct sum of type I_n's. If we know that the restriction of G_F to each summand is of finite order, then the same will follow for G_F. So it will suffice to assume that G_F is of type I_n. By Lemma 4.3, there exists a freely acting finite group K of order n such that $[K] = [G_F]$. We can assume that $F = F^{-1}$ and that the identity lies in F, so that G_F is the multiplicative semigroup generated by F, By Lemma 3.1, we may represent each α in F in the form $\alpha = \sum_k Q_k^{(\alpha)} k$. Let $\mathfrak{B}$ be the smallest K-invariant boolean algebra of projections containing all the $Q_k^{(\alpha)}$. $\mathfrak{B}$ is obviously finite, as is the collection of all linear endomorphisms of M of the form $\sum_k R_k k$ $(R_k \in \mathfrak{B})$. But all products of the α in F lie in this collection. Therefore, G_F is finite.

We conclude with a result on the imbedding of bounded type I's in type I_n's.

LEMMA 4. 5. *Let K be a bounded type I subgroup of a type II group G. Then for an appropriate s, there exists a type I_s subgroup L of $[G]$ such that $K \subset [L]$.*

Proof. To begin, suppose that K is a type I_n subgroup of $[G]$, and that $m = nr$ is an integer divisible by n. We will construct a type I_m subgroup L of $[G]$ such that $K \subset [L]$. Replacing K by an equivalent group if necessary, we can assume that K is freely acting. Choose a projection P such that the kP $(k \in K)$ form an abelian basis for K. Denote by Z the fixed algebra of G, and applying Maharam's lemma, partition $P = P_0 + \cdots + P_{r-1}$ as a sum of mutually orthogonal projections with $E_Z(P_i) = 1/m$. By Lemma 3. 3, choose an α in $[G]$ such that $\alpha(P_i) = P_{i+1}$ (indices mod r), $\alpha^r =$ identity, $\alpha =$ identity off P. Next, define an automorphism β in $[G]$ as follows: if $Q \leqq kP$, then $\beta Q = k\alpha k^{-1}Q$. Let L be the group generated by K and β. It is easy to see that β commutes with each element of K, so elements of L have the form $k\beta^i$. Further, $\sum_k \sum_{i=0}^{r-1} k\beta^i P_0 = I$. Now L is freely acting: if not, then some $k_0\beta^{i_0} \neq e$ will certainly leave fixed a non-zero projection of the form $k_1\beta^{i_1}R$ $(R \leqq P_0)$. This gives $k_0k_1\beta^{i_0+i_1}R = k_1\beta^{i_1}R$. The left side is $\leqq k_0k_1P$, the right $\leqq k_1P$, and hence $k_0 = e$, and $\beta^{i_0+i_1}R = k_1\beta^{i_1}R$. This gives $\alpha^{i_0}R$, implying $i_0 = 0 \pmod r$ and $k_0\beta^{i_0} =$ identity, a contradiction. Therefore, L is a freely acting group of type I_m. Any projection in the fixed algebra of L has the form $\sum_k \sum_{i=0}^{r-1} k\beta^i R$, for $R \leqq P_0$, and such a projection is obviously invariant under K. This implies that $K \subset [L]$, and the first assertion is established.

In the general case, there will exist mutually orthogonal projections $C_1, \cdots, C_t$ in the fixed algebra of K such that $I = \sum C_i$ and $[K]_{C_i}$ on C_iM is of type I_{n_i}. Let $s =$ least common multiple of the n_i. Because $[G]_{C_i}$ is of type II (Lemma 3. 5), we can apply the above construction to each $[K]_{C_i}$ on C_iM, imbedding these in type I_s subgroups L_i of $[G]_{C_i}$ on C_iM. Now, $L = \sum L_i$ is a type I_s subgroup of $[G]$ and $K \subset [L]$. This proves the lemma.

5. Approximately finite groups. We prepare now to confront our main problem, approximation of arbitrary MP automorphisms in type I subgroups. The initial step concerns a relaxation of conditions in Lemma 4. 2. According to that lemma, if K is a type I group, then any MP automorphism

α which leaves the fixed algebra Z_K of K pointwise fixed is already in $[K]$. This is generalized here to a statement that, if an MP automorphism α leaves Z_K "almost pointwise fixed," then α is "almost in $[K]$."

A numerical lemma, useful in several other connections, will provide the decisive estimate.

LEMMA 5.1. *Let (a_{ij}) be an $n \times n$ matrix with real entries. Assume that for each subset S of $\Lambda = (1, \cdots, n)$*

$$|\sum_{i \in S,\ j \in \Lambda - S} a_{ij}| < \epsilon. \tag{5.1}$$

Then $|\sum_{i \neq j} a_{ij}| < 4\epsilon$.

Proof. We can assume that n is a power of 2. For choose m such that $2^m > n$, and set $a_{ij} = 0$ whenever $n + 1 \leqq i \leqq 2^m$ or $n + 1 \leqq j \leqq 2^m$. The inequality (5.1) holds for the enlarged matrix, and the sum of off-diagonal terms remains unchanged. In what follows, then, we take $\Lambda = (1, \cdots, 2^m)$.

Partition Λ into two disjoint subsets Λ_0, Λ_1, each with 2^{m-1} elements, in such a way that the sum $s(0,1) = \sum_{i \in \Lambda_0,\ j \in \Lambda_1} (a_{ij} + a_{ji})$ is a maximum among corresponding sums for all such partitions of Λ. Denote by Δ_r the set of all r-tuples $(\epsilon_1 \cdots \epsilon_r)$, where $\epsilon_i = 0$ or 1. If the partition $\Lambda = \bigcup_{\delta \in \Delta_r} \Lambda_\delta$ is defined for $r < m$, with $|\Lambda_\delta| = 2^{m-r}$, we partition each Λ_δ into disjoint subsets $\Lambda_{\delta 0}$, $\Lambda_{\delta 1}$, each with 2^{m-r-1} elements, in such a way that

$$s(\delta 0, \delta 1) = \sum_{i \in \Lambda_{\delta 0},\ j \in \Lambda_{\delta 1}} (a_{ij} + a_{ji}) \tag{5.2}$$

is a maximum among corresponding sums for all such partitions of Λ_δ. Let $A_{r+1} = \sum_{\delta \in \Delta_r} s(\delta 0, \delta 1)$. Then

$$\sum_{i \neq j} a_{ij} = \sum_{r=1}^{m} A_r \text{ and } A_1 < 2\epsilon. \tag{5.3}$$

Now, we assert, $A_r \geqq 2A_{r+1}$, for each $r < m$. To see this, we apply the maximum property of the sums $s(\delta, \delta') = s(\delta', \delta)$ to compute

$$\begin{aligned}
2A_r &= 2 \sum_{\delta \in \Delta_{r-1}} s(\delta 0, \delta 1) \\
&= 2 \sum_{\delta \in \Delta_{r-1}} [s(\delta 00, \delta 10) + s(\delta 00, \delta 11) + s(\delta 01, \delta 10) + s(\delta 01, \delta 11)] \\
&= \sum_{\delta \in \Delta_{r-1}} [s(\delta 00, \delta 01) + s(\delta 00, \delta 10) + s(\delta 11, \delta 01) + s(\delta 11, \delta 10)] \\
&= \sum_{\delta \in \Delta_{r-1}} [s(\delta 00, \delta 01) + s(\delta 00, \delta 11) + s(\delta 10, \delta 01) + s(\delta 10, \delta 11)] \\
&= 2 \sum_{\delta \in \Delta_{r-1}} [s(\delta 00, \delta 01) + s(\delta 10, \delta 11)] + A_r = 2A_{r+1} + A_r,
\end{aligned}$$

establishing the inequality. Therefore,

$$A_1 \geqq 2A_2 \geqq \cdots \geqq 2^{m-1}A_m, \text{ and } \sum_{r=1}^{m} A_r \leqq \sum_{r=1}^{m} A_1/2^{r-1} < 2A_1 < 4\epsilon.$$

Application of the same argument to the matrix $(-a_{ij})$ completes the proof.

LEMMA 5.2. *Let K be a type I group with fixed algebra denoted Z, and let α be an MP automorphism of M such that $F(\alpha,\beta) = 0$, for all $\beta \in K$. Then*

$$\sup_{C \in Z_P} \lambda(C \Delta \alpha C) \geqq \tfrac{1}{2}. \tag{5.4}$$

Proof. (Recall, throughout, that the measure λ is normalized by $\lambda(I) = 1$. The Δ in (5.4) of course denotes symmetric difference.) The proof depends on the following fact:

(5.5) given $C \neq 0$ in Z_P, there exists a non-zero D in Z_P, $D \leqq C$, such that $D\alpha D = 0$.

Assertion (5.5) will be established by an indirect argument: assume some non-zero C_0 in Z_P has the property that $D\alpha D \neq 0$, for each non-zero $D \leqq C_0$, D in Z. Using type I theory, we choose an F in Z_P such that $FC \neq 0$ and $[K]_F$ on FM is of type I_n, for an appropriate n. Write $F = P_1 + \cdots + P_n$, where the P_i are abelian over Z and have the same expectation relative to Z.

Assume that for each i and each non-zero $E \leqq C_0F$, $E \in Z$, there exists a non-zero C in Z, $C \leqq E$, such that $C\alpha(C)P_i = 0$. In particular then we can choose a non-zero $C_1 \leqq C_0F$ such that $C_1\alpha(C_1)P_1 = 0$, a non-zero, $C_2 \leqq C_1$ such that $C_2\alpha(C_2)P_2 = 0$, etc., arriving finally at a non-zero $C_n \leqq C_0F$ such that $C_n\alpha(C_n)P_i = 0$, for all i. This gives

$$C_n\alpha(C_n) = C_n\alpha(C_n)F = \sum_i C_n\alpha(C_n)P_i = 0.$$

This contradicts the basic assumption in our indirect proof. Therefore, there exists an i, which we take as 1, and a non-zero E in Z, $E \leqq C_0F$, such that $C\alpha(C)P_1 \neq 0$, for all non-zero $C \leqq E$. We will have $\alpha(C)P_1 \geqq CP_1$, for all $C \leqq E$; otherwise, for some such C, $CP_1(I - \alpha(C)P_1) \neq 0$, and if we choose D in Z_P so that $\alpha(C)P_1 = DP_1$, then $C(I-D)P_1 = CP_1(I-\alpha(C)P_1)$, whence $C(I-D) \neq 0$, because C is dominated by the carrier F of P_1; now on the one hand, $[C(I-D)]\alpha[C(I-D)]P_1 \neq 0$, by choice of the pair (E, P_1), but on the other hand, $[C(I-D)]\alpha[C(I-D)]P_1 \leqq [C(I-D)]\alpha(C)P_1 = C(I-D)DP_1 = 0$, a contradiction. Further, if we choose projections D_i

in Z, $D_i \leqq F$, such that $\alpha(P_i)P_1 = D_iP_1$, then for some i, $D_iE \neq 0$, for otherwise $E\alpha(F)P_1 = 0$, whence $E\alpha(E)P_1 = 0$, again a contradiction.

Now consider any C in Z, $C \leqq D_iE \neq 0$. Then $\alpha(CP_i)P_1 = \alpha(C)D_iP_1 \geqq CD_iP_1 = CP_1$. Therefore $\alpha(CP_i) \geqq CP_1$, and equality must hold because these projection have the same measure. It follows that $\alpha(CP_i) = CP_1$, for all $C \leqq D_iE \neq 0$. Because the abelian projections P_1 and P_i have the same expectation relative to Z, there exists a β in $[K]$ such that $\beta(P_i) = P_1$. Also $\beta(CP_i) = CP_1$, for all $C \leqq D_iE$, C in Z, and this shows that $D_iEP_i \leqq F(\alpha, \beta)$. But $D_iEP_i \neq 0$, because P_i has Z-carrier $F \geqq D_iE$. Therefore $F(\alpha, \beta) \neq 0$, for some β in $[K]$, hence for some β' in K, a contradiction, and (5.5) is established.

Turning to the lemma itself, we apply (5.5) to express I as a (necessarily countable) sum of mutually orthogonal non-zero projections D_i in Z satisfying $D_i\alpha D_i = 0$, for each i. Fix a $\delta > 0$. Choose n so that $\sum_{k=n}^{\infty} \lambda(D_k) < \delta$, and define $C_i = D_i$ $(i < n)$, $C_n = \sum_{i \geqq n} D_i$. Let

$$k = \sup{}_{C \in Z_P} \lambda(C\Delta\alpha C) = \sup{}_{C \in Z_P} \lambda[\alpha(C)(I - C) + C\alpha(I - C)].$$

Let $a_{ij} = \lambda[\alpha(C_i)C_j + C_i\alpha(C_j)]$, for $1 \leqq i, j \leqq n$. Then if $\Lambda = (1, \cdots, n)$, and $C = \sum_{i \in S} C_i$, we have $\sum_{i \in S,\ j \in \Lambda - S} a_{ij} = \lambda[\alpha(C)(I - C) + C\alpha(I - C)] \leqq k$. By Lemma 5.1, $\sum_{i \neq j} a_{ij} \leqq 4k$. But

$$\sum_i a_{ii} = \sum_i 2\lambda(\alpha(C_i)C_i) = 2\lambda(\alpha(C_n)C_n) < 2\delta,$$

and

$$\sum_{i,j} a_{ij} = 2\lambda(I) = 2 = \sum_i a_{ii} + \sum_{i \neq j} a_{ij} \leqq 2\delta + 4k.$$

Therefore, $k \geqq (1 - \delta)/2$, and since δ is arbitrary, $k \geqq \frac{1}{2}$.

LEMMA 5.3. *Let K be a type I group with fixed algeba Z, and let α be an arbitrary MP automorphism of M. Assume that* $\sup_{C \in Z_P} \lambda(C\Delta\alpha C) < \epsilon$. *Then*

$$\lambda(E([K], \alpha)) > 1 - 2\epsilon. \tag{5.6}$$

Proof. Write $E = E([K], \alpha)$. By definition, there exists a β in $[K]$ such that $E\alpha(P) = E\beta(P)$, for all P in M. Let $\tau = \alpha\beta^{-1}$. Then $\tau E = E$, τ leaves E absolutely fixed, and $F(\tau, \gamma) \leqq E$, for all $\gamma \in [K]$: in fact, $E\alpha P = E\beta P$ for all P implies $E\tau P = EP$ for all P, so in particular $P \leqq E$ gives $P = E\tau P \leqq \tau P$, forcing $P = \tau P$; and applying Lemma 3.4, we have for any γ in $[K]$, $F(\tau, \gamma) = F(\gamma, \alpha\beta^{-1}) = \beta F(\gamma\beta, \alpha) \leqq \beta\alpha^{-1}E = \tau^{-1}E = E$. Con-

sider the restricted group $[K]_{(I-E)}$ on $(I-E)M$. If we denote by Z_0 the fixed algebra of $[K]_{(I-E)}$ on $(I-E)M$, then Lemma 5.2 gives

$$\sup_{C\in Z_0}\lambda(C\Delta\tau C)\geqq\lambda(I-E)/2.$$

Now by Lemma 3.5, $Z_0=Z(I-E)$. Also, for any C in Z, $\alpha C=\tau C=\tau(C(I-E))+CE$. Therefore,

$$\lambda(I-E)/2\leqq\sup_{C\in Z_0}\lambda(C\Delta\tau C)=\sup_{C\in Z}\lambda(C\Delta\tau C)=\sup_{C\in Z}\lambda(C\Delta\alpha C)<\epsilon,$$

so $1-\lambda(E)<2\epsilon$, and $\lambda(E[K],\alpha))=\lambda(E)>1-2\epsilon$.

Application of Lemma 5.3 in the case $K=$ identity yields a useful result of Halmos [3] on the equivalence of two natural metrics on the group of all MP automorphisms, which we discuss now in the current notation. The standard metric on the group of all MP automorphisms of M is defined by

$$d(\alpha,\beta)=\sup_{P\in M_P}\lambda(\alpha P\Delta\beta P). \tag{5.7}$$

Endowed with d, this group is a complete metric space, in which the natural notion of distance from an automorphism α to a full subgroup $[G]$ is given by

$$d(\alpha,[G])=\inf_{\gamma\in[G]}d(\alpha,\gamma). \tag{5.8}$$

On the other hand, an apparently more revealing metrization of the group of all measure preserving automorphism is available. Expressly, define

$$\delta(\alpha,\beta)=\lambda(I-F(\alpha,\beta)). \tag{5.9}$$

It is easy to see that δ is a metric, the triangle inequality following from the relation $F(\alpha,\beta)F(\beta,\gamma)\leqq F(\alpha,\gamma)$. Like d, the metric δ is invariant: $\delta(\alpha,\beta)=\delta(\alpha\gamma,\beta\gamma)=\delta(\gamma\alpha,\gamma\beta)$, for all MP automorphism α, β, γ, this because $F(\alpha,\beta)=F(\gamma\alpha,\gamma\beta)=\gamma F(\alpha\gamma,\beta\gamma)$. For any MP group G, we have $\inf_{\gamma\in[G]}\delta(\alpha,\gamma)=1-\sup_{\gamma\in[G]}\lambda(F(\alpha,\gamma))=1-\sup_{\gamma\in[G]}\lambda(\alpha F(\alpha,\gamma))$, and by formula (3.2) this becomes

$$\delta(\alpha,[G])=\lambda(I-E([G],\alpha)). \tag{5.10}$$

As noted by Halmos, the key fact is that these metrics can be used interchangeably:

Lemma 5.4. *The metrics d and δ are equivalent, and any full group is complete in either metric.*

Proof. First we note that d is stronger than δ:

$$\begin{aligned}\lambda(\alpha P\Delta\beta P)&=\lambda(\alpha[P(I-F(\alpha,\beta))]\Delta\beta[P(I-F(\alpha,\beta))])\\&=\lambda[(P\Delta\alpha^{-1}\beta P)(I-F(e,\alpha^{-1}\beta)]\leqq\delta(\alpha,\beta),\end{aligned}$$

so that $d(\alpha, \beta) \leqq \delta(\alpha, \beta)$. On the other hand, applying Lemma 5.3 when K consists of the identity alone, and therefore $Z = M$ and $E([K], \alpha) = F(e, \alpha)$, we see that $d(e, \alpha) < \epsilon$ implies $\lambda(I - F(e, \alpha)) < 2\epsilon$, so that $\delta(e, \alpha) < 2\epsilon$. This and the invariance of the metrics d and δ now show that the identity map from any (G, d) to (G, δ) is uniformly continuous, proving that the metrics are equivalent. If α_n is a δ-cauchy sequence in a full group $[G]$, then α_n is automatically d-cauchy, and therefore converges in d-metric to some MP automorphism α. By equivalence, this convergence carries over to the δ-metric. But then, α lies in $[G]$, for $\lim_n \lambda(F(\alpha, \alpha_n)) = 1$ clearly entails $\mathrm{LUB}_{\gamma \in [G]} F(\alpha, \gamma) = I$, that is, $\alpha \in [G]$. Again by equivalence, $[G]$ is also complete in d.

[The fact that δ is stronger than d can of course be proved rather easily without benefit of Lemma 5.3. One procedure is this: let $\tau = \alpha^{-1}\beta$, $F = F(e, \tau)$, and choose a P maximal with the property that $P\tau P = 0$. Then $I = F + [\tau^{-1}P \cup (P + \tau P)]$, and

$$\delta(\alpha, \beta) = \lambda(I - F) \leqq \tfrac{3}{2}\lambda(P \Delta \tau P) \leqq \tfrac{3}{2} d(\alpha, \beta).]$$

PROPOSITION 5.1. *The following conditions on a group G of MP automorphisms are equivalent: for each finite set $\beta_1, \cdots, \beta_n$ in G and each $\epsilon > 0$,*

(1) *there exists a type I subgroup K of $[G]$ such that $\delta(\beta_j, [K]) < \epsilon$, for $i = 1, \cdots, n$;*

(2) *there exists a finite subgroup K of $[G]$ and elements $\beta'_1, \cdots, \beta'_n$ of K such that $d(\beta_i, \beta'_i) < \epsilon$, for $i = 1, \cdots, n$;*

(3) *there exists a type I subgroup K of $[G]$ such that*

$$\sup_{C \in Z_K} \lambda(C \Delta \beta_i C) < \epsilon,$$

for $i = 1, \cdots, n$, where Z_K denotes the fixed algebra of K.

Further, the validity of these conditions for G entails their validity for $[G]$, and therefore, for any group equivalent to G.

Proof. (1) implies (2). Trivially, one can assume that the K in condition (1) is of bounded type I. This done, let β'_i be an element of K such that $\delta(\beta_i, \beta'_i) < \epsilon$, so $d(\beta_i, \beta'_i) < \epsilon$. By Lemma 4.4, the group generated by the β'_i is finite, and (2) follows.

(2) implies (3). Let C lie in the fixed algebra of the group K of condition (2). Then

$$\lambda(\beta_i C \Delta C) \leqq \lambda(\beta_i C \Delta \beta'_i C) + \lambda(\beta'_i C \Delta C) = \lambda(\beta_i C \Delta \beta'_i C)$$
$$\leqq \sup_{P \in M_P} \lambda(\beta_i P \Delta \beta'_i P) = d(\beta_i, \beta'_i) < \epsilon.$$

(3) implies (1). This follows immediately from Lemma 5.3.

Turning to the last statement of the proposition, we assume condition (1) holds for elements of G, and prove that it will then hold for arbitrary $\beta_1, \cdots, \beta_n$ in $[G]$. For this, we represent $\beta_i = \sum_{k=1}^{\infty} Q_k^{(i)} \alpha_k^{(i)}$, by formula (3.1), where the $\alpha_k^{(i)} \in G$ and the sets $Q_k^{(i)}$ satisfy the orthogonality conditions of Lemma 3.1. Fix a $\delta > 0$. Choose an integer r such that $\lambda(\sum_{k \leqq r} Q_k^{(i)}) > 1 - \delta/2$, for all i. Applying condition (1), choose a type I subgroup K of $[G]$ such that $\delta(\beta, [K]) < \delta/2mn$, for each α in the set

$$F = [\alpha_k^{(i)} \mid 1 \leqq i \leqq n, 1 \leqq k \leqq r].$$

Define $E = \prod_{\alpha \in F} E([K], \alpha)$. It is easy to see that $\lambda(E) \geqq 1 - \delta/2$. For each α in F, denote by $\gamma(\alpha)$ the element of $[K]$ such that $E([K], \alpha)\alpha = E([K], \alpha)\gamma(\alpha)$. Then $E\alpha = E\gamma(\alpha)$, for all α, so $E(\sum_{k=1}^{r} Q_k^{(i)} \alpha_k^{(i)}) = \sum_{k=1}^{r} Q_k^{(i)} E\gamma(\alpha_k^{(i)})$ for all i. Lemma 3.4 now shows that $E([K], \beta_i) \geqq \sum_{k=1}^{r} Q_k^{(i)} E$. Therefore, $\lambda(E[K], \beta_i))$ $\geqq \lambda((\sum_{k=1}^{r} Q_k^{(i)}) E) \geqq 1 - \delta$. This completes the proof.

Definition 5.1. The group G is called *approximately finite* if it satisfies any one of the equivalent condition (1)-(3) of Proposition 5.1.

Automatically, any type I group is approximately finite. Interest centers, of course, on approximately finite groups of type II. An example of an approximately finite group of type II—which serves as a prototype in subsequent developments—can be obtained as follows. Let A be an infinite index set, and for each $a \in A$, let G_a be an abstract group of order 2. Form the restricted direct product $\prod_a G_a = G$ of the G_a (where it is understood that all but a finite number of components of each g in G are identities). Lemmas 2.1 assures us that G has a faithful representation as a freely-acting group of MP automorphisms of an abstract non-atomic hyperstonian measure space. In this representation, G will automatically be approximately finite, for any finite subset of G generates a finite, and therefore type I, subgroup of G. Another class of examples of more classical interest is developed by

THEOREM 1. *Any singly-generated group of MP automorphism is approximately finite.*

Proof. Let α be an MP automorphism of M, and G the group of MP automorphisms generated by α. The following assertion affords the basis of proof:

(5.11) Let E be a non-zero projection which dominates no α-fixed projections. Then there exists a β in $[G]$ such that $\beta=\alpha$ on E, $\beta=$ identity off $E\cup\alpha E$, and β generates a type I subgroup of $[G]$.

First, we partition E into a possibly terminating sum $E=\sum P_n$ of mutually orthogonal projections P_n which satisfy $\alpha P_1=(\alpha E)(I-E)$ and $\alpha P_{n+1}\leqq P_n$, for $n\geqq 1$. To do this, define $P_1=E\alpha^{-1}(I-E)$, $P_0=\alpha P_1$, and for $n\geqq 1$, $P_{n+1}=[E-(P_1+\cdots+P_n)]\alpha^{-1}(P_1+\cdots+P_n)$. By construction, the P_n are mutually orthogonal. Now if $R\leqq P_{n+1}$ and $\alpha R\leqq P_i$ $(0<i\leqq n)$, then $R\leqq(\alpha^{-1}P_i)(E-(P_1+\cdots+P_i))\leqq P_{i+1}$, forcing $i=n$. Therefore $\alpha P_{n+1}\leqq P_n$. If $P_{n+1}=0$, then $E-(P_1+\cdots+P_n)$ is an α-fixed projection $\leqq E$, and our assumptions force $E=P_1+\cdots+P_n$. In the same fashion, it follows that if $P_{n+1}\neq 0$ for all n, then $E=\sum_{n=1}^{\infty}P_n$.

Define $Q_n=P_n-\alpha P_{n+1}$ $(n\geqq 1)$. We have $P_0=\sum_{n\geqq 1}\alpha^n Q_n$. Moreover, the projections $\alpha E, Q_1, Q_2,\cdots, I-(E+P_0)$ are mutually orthogonal with LUB I, as are the projections E, $\alpha Q_1, \alpha^2 Q_2,\cdots, I-(E+P_0)$. Therefore, by Lemma 3.1, the formula

$$(5.12)\qquad \beta(P)=\alpha(E)\alpha(P)+\sum_n Q_n\alpha^{-n}(P)+[I-(E+P_0)]P$$

defines an element of $[G]$ which agrees on E with α. Now if $R\leqq Q_n$, then $\beta^k R=\alpha^k R$ $(k\leqq n)$ and $\beta^{n+1}R=\beta(\alpha^n R)=Q_n R=R$. This shows that the projection $R_1=\sum_{k=0}^{n}\beta^k R$ is β-fixed and $RQ_n=R_1Q_n$. Therefore, Q_n is abelian relative to β. Therefore, all projections $\alpha^i Q_n$ $(i\leqq n)$ are abelian relative to β. But $\sum_{n\geqq 1}\sum_{k=0}^{n}\alpha^k Q_n=E+P_0$, and the complement of $E+P_0$ is automatically abelian relative to β. It follows that the group generated by β is of type I, and (5.11) is verified.

Turning to the theorem itself, we have noted in Section 2 that $[G]$ is the direct sum of a type I and a type II group, and in the present situation, it is clear that these summands are the full groups generated by restrictions of α. It will clearly suffice, therefore, to assume that G is of type II. This done,

denote by Z the fixed algebra of G, and corresponding to $\delta > 0$, choose a projection E in M such that $E_Z(E) = 1 - \delta$ (this by Maharam's lemma). By this construction, $\lambda(I - E) < \delta$, and E dominates no α-fixed projections (save 0). Apply (5.11) to this E. If K denotes the type I group generated by the β of (5.11), then

$$d(\alpha, [K]) \leqq d(\alpha, \beta) = \sup_P \lambda(\alpha P \Delta \beta P)$$
$$= \sup_P \lambda((\alpha P)(I - E) \Delta (\beta P)(I - E)) \leqq 2\lambda(I - E) < 2\delta.$$

If k is any positive integer, then the triangle inequality and the invariance of d give $d(\alpha^k, \beta^k) \leqq \sum_{r=0}^{k-1} d(\alpha^{k-r}\beta^r, \alpha^{k-(r+1)}\beta^{r+1}) < 2k\delta$, and $d(\alpha^{-k}, \beta^{-k}) = d(\alpha^k, \beta^k) < 2k\delta$. It follows therefore that for any $\epsilon > 0$ and any finite subset F of G, there exists a type I subgroup K of G such that $d(\gamma, [K]) < \epsilon$, for all $\gamma \in F$, and hence $\delta(\gamma, [K]) < 2\epsilon$. Thus condition (1) of Proposition 5.1 is verified, and by definition, G is approximately finite.

LEMMA 5.5. *For any MP automorphism α and arbitrary MP groups G_1 and G_2, $E([G_1], \alpha) E([G_2], \alpha) = E([G_1] \cap [G_2], \alpha)$.*

Proof. Write $E_i = E([G_i], \alpha)$, and choose α_i in $[G_i]$ such that $E_i\alpha_i = E_i\alpha$. We have $E_1E_2\alpha = E_1E_2\alpha_1 = E_1E_2\alpha_2$. The main step consists in showing that there exists a γ in $[G_1] \cap [G_2]$ such that $E_1E_2\gamma = E_1E_2\alpha_1 = E_1E_2\alpha_2$. To this end, write $E' = \alpha_1^{-1}(E_1E_2) = \alpha_2^{-1}(E_1E_2)$, and note that α_1 and α_2 agree on E'. Let E'_0 be the maximal α_1-fixed projection under E'. Let $E = E' - E'_0$, and construct the β of (5.11) for the pair (E, α_1). From the fact that $\alpha_1 = \alpha_2$ on E, it is easy to conclude that the formula (5.12) defining β in terms of α_1 remains valid when α_1 is replaced by α_2. It follows that $\beta \in [G_1] \cap [G_2]$. Now let $\gamma = \beta$ on $E \cup \alpha_1 E$, $\gamma = \alpha_1$ (and hence α_2) on E'_0, $\gamma =$ identity elsewhere. Then $\gamma \in [G_1] \cap [G_2]$ and $\gamma = \alpha_1 = \alpha_2$ on E'. Now for all P, $\gamma(E'P) = \alpha_1(E'P) = E_1E_2\alpha_2(P) = E_1E_2\alpha_2(P)$. This proves that $E_1E_2 \leqq E([G_1] \cap [G_2], \alpha)$. Automatically $E([G_1] \cap [G_2], \alpha)$ is dominated by each E_i. Therefore, $E([G_1] \cap [G_2], \alpha) = E_1E_2$, and the lemma is proved.

With this, it is easy to establish

THEOREM 2. *Any subgroup of an approximately finite group is itself approximately finite.*

Proof. Let G be an approximately finite group, and let K be any subgroup of $[G]$. Let F be a finite subset of K, and take $\epsilon > 0$. There exists a type I subgroup L of $[G]$ such that $\lambda(E([L], \alpha) > 1 - \epsilon$, for all α in

F. Applying Lemma 5.5 and the fact that $E([K],\alpha)=I$, we obtain $\lambda(E([K]\cap[L],\alpha))=\lambda(E([L],\alpha))>1-\epsilon$. Since any subgroup of a type I group is itself of type I, it follows that $[L]\cap[K]$ is a type I subgroup of $[K]$. This proves that K is approximately finite.

In particular, therefore, any local subgroup $[G]_P$ of the full group determined by an approximately finite group is approximately finite. Conversely,

COROLLARY 5.1. *Approximate finiteness is a local property: if G is an MP automorphism group with fixed algebra Z, and if for some projection P in M, $[G]_P$ is approximately finite, then so is $[G]_{\bar{P}}$, where $\bar{P}$ denotes the the Z-carrier of P.*

Proof. Plainly, we can assume that G is of type II and that $\bar{P}=I$. For each $\delta>0$, there exists a projection C in Z such that $\lambda(C)>1-\delta$ and $E_Z(P)$ is bounded away from 0 on C. Granting we have proved $[G]_C$ approximately finite, for each such C, then it will clearly follow that $[G]$ is itself approximately finite. Therefore, we can assume $E_Z(P)\geqq 1/n$, for some integer n. This done, apply Maharam's lemma to choose mutually orthogonal projections $P_0,\cdots,P_{n-1}$ such that $E_Z(P_i)=1/n$, for each i, whence $\sum_{i=0}^{n-1}P_i=I$. By Lemma 3.2, given i, there exists a ρ in $[G]$ such that $\rho P_i\leqq P$. It follows that $\rho[G]_{P_i}\rho^{-1}\subset[G]_P$, so by Theorem 2, $\rho[G]_{P_i}\rho^{-1}$ and therefore $[G]_{P_i}$ is approximately finite. Let

$$[G]_{P_0,\cdots,P_{n-1}}=[\beta\in[G]\mid\beta P_i=P_i \text{ for each } i].$$

This group will be approximately finite, being a direct sum of the approximately finite groups $[G]_{P_i}$ on P_iM. By Lemma 3.3, there exists an α in $[G]$ such that $\alpha P_i=P_{i+1}$ (indices $\bmod n$) and $\alpha^n=$ identity. Further, let $G_0=[\beta\in[G]_{P_0,\cdots,P_{n-1}}\mid\beta\alpha=\alpha\beta]$. For each γ in $[G]_{P_0,\cdots,P_{n-1}}$ and each i, the automorphism

$$\gamma'(Q)=\sum_{j=0}^{n-1}\alpha^j[P_i\gamma(\alpha^{-j}(Q))] \tag{5.13}$$

lies in G_0 and agrees with γ on all projections dominated by P_i. Therefore, $E([G_0],\gamma)\geqq P_i$ for all i, showing that $E([G_0],\gamma)=I$, $\gamma\in[G_0]$, and $[G_0]=[G]_{P_0,\cdots,P_{n-1}}$. Let K denote the group generated by α and G_0. Application of Lemma 3.5 shows that the fixed algebra Z_K of K coincides with Z. Given an arbitrary γ in $[G]$, Lemma 3.2 and the fact $Z=Z_K$ show that $[K]$ will contain an element μ such that $\mu^{-1}\gamma P_i=P_i$, for all i

simultaneously. Therefore, $\mu^{-1}\gamma \in [G]_{P_0,\cdots,P_{n-1}} = [G_0] \subset [K]$, so $\gamma \in [K]$, and $[G] = [K]$.

The problem is now reduced to showing that K is approximately finite. For this, it will suffice to prove the following: given $\beta_1, \cdots, \beta_r$ in G_0 and $\epsilon > 0$, there exists a finite subgroup S of $[G]$ containing α and containing element β''_i $(1 \leqq i \leqq r)$ such that $d(\beta_i, \beta''_i) < \epsilon$. To construct this S, choose a finite subgroup S_0 of $[G]_{P_0}$ containing elements β'_i $(1 \leqq i \leqq r)$ such that $\sup_{P \leq P_0} \lambda(\beta_i(P) \Delta \beta'_i(P)) < \epsilon/n$. As in (5.13), set $\beta''_i = \sum_k \alpha^k [P_0 \beta'_i(\alpha^{-k}(\cdot))]$. Each β''_i commutes with α, and α and the β''_i generate a finite subgroup of $[G]$. Now, for any P in M,

$$\lambda(\beta''_i(P) \Delta \beta_i(P)) = \sum_k \lambda(\alpha^k(P_0\beta'_i(\alpha^{-k}P)) \Delta \alpha^k(P_0\beta_i(\alpha^{-k}P)))$$
$$= \sum_k \lambda(\beta'_i(P_0\alpha^{-k}P) \Delta \beta_i(P_0\alpha^{-k}P)) < n(\epsilon/n) = \epsilon.$$

This concludes the proof.

6. The structure of approximately finite groups. As noted earlier, a restricted direct product $\prod_{a \in A} G_a$ of groups of order two is approximately finite in any faithful free action. One such action, of particular significance, can be realized as follows. Consider each G_a as a two-point measure space, and form the measure space (S, m) consisting of the direct product of these two-point measure spaces and an arbitrary finite measure space (the latter to appear as a fixed algebra). The generator of each G_a determines an involution of (S, m), and together these involutions generate a group of MP transformations of (S, m) which, algebraically, is isomorphic to the original product group. Passage to the hyperstonian measure space associated with (S, m) represents this group, in the customary setting of this theory, as a group of MP automorphisms. Now essentially, our main objective is to show that this example is canonical: subject to certain natural countability conditions, an arbitrary type *II* approximately finite automorphism group is equivalent to the automorphism group arising in the above construction with A countably infinite. [In this equivalence theory, to avoid rather unrewarding complications, we do not attempt to discuss cases involving either non-countable groups or measure algebras with bases of arbitrary cardinality. It is of interest that, in the parallel W^*-algebra theory of approximate finiteness, the difficulties atending the non-separable cases have been resolved by Misonou [7].]

For notation in the following, G will denote a type *II* group of MP automorphisms of (M, λ) with fixed algebra Z.

LEMMA 6.1. *Assume G approximately finite. Let K be a finite freely acting subgroup of $[G]$, and α an arbitrary element of $[G]$. Then, given $\epsilon > 0$, there exists a type I_n subgroup L of $[G]$ such that $K \subset [L]$ and $\lambda(E([L], \alpha)) > 1 - \epsilon$.*

Proof. Corresponding to $\delta > 0$ (to be specified later), choose a bounded type I subgroup L_1 of $[G]$ such that $\lambda(E([L_1], \gamma)) > 1 - \delta$, where γ runs over the finite set $F = \{K, \alpha\}$.

Let Z_K be the fixed algebra of K, and $n =$ order K. We assert: if P is any projection with $\lambda(I - P) < \delta$, then there exists a projection C in Z_K, $C \leqq P$, such that $\lambda(I - C) < n\delta$. To see this, let $P_1, \cdots, P_n$ be an abelian base for K over Z_K, and write $P = \sum_i C_i P_i$ $(C_i \in Z_K)$. Let $C = \prod_{i=1}^{n} C_i$. Then,

$$\lambda(C) \geqq 1 - \sum_{i=1}^{n} \lambda(I - C) = -(n-1) + n[(1/n) \sum_i \lambda(C_i)]$$
$$= 1 - n\lambda(I - P) > 1 - n\delta,$$

as asserted.

Define $E = \prod_{\gamma \in F} E([L_1], \gamma)$. Clearly, $\lambda(E) > 1 - (n-1)\delta$. By the above, we can choose a C in Z_K such that $C \leqq E$ and $\lambda(C) > 1 - n(n+1)\delta$. For each γ in F, there exists a γ_1 in $[L_1]$ such that $C\gamma(P) = C\gamma_1(P)$, for all P. In particular, $C\alpha(P) = C\alpha_1(P)$, α_1 in $[L_1]$. We claim, an α_2 in $[L_1]$ exists such that α_2 leaves $I - C$ absolutely fixed and $D\alpha_1 = D\alpha_2$, for some $D \leqq C$, with $\lambda(D) > 1 - 2n(n+1)\delta$. In fact, set $D = C\alpha_1(C)$. Now

$$E_{Z_{L_1}}(C\alpha_1(I - C)) = E_{Z_{L_1}}((\alpha_1 C)(I - C)),$$

so by Lemma 3.2, $[L_1]$ contains a ρ such that $\rho[(\alpha_1 C)(I - C)] = C\alpha_1(I - C)$, $\rho^2 =$ identity, and $\rho =$ identity off $C \Delta \alpha_1 C$. Then

$$(\rho\alpha_1)C = \rho[(\alpha_1 C)(I - C) + (\alpha_1 C)C] = C\alpha_1 C + C\alpha_1(I - C) = C,$$

and if we set $\alpha_2 = \rho\alpha_1$ on C, $\alpha_2 =$ identity on $(I - C)$, then $D\alpha = D\alpha_1 = D\alpha_2$ and $\lambda(D) > -1 - 2\lambda(I - C) > 1 - 2n(n+1)\delta$. Denote by L_2 the group generated by K and α_2. This group has a fixed algebra containing $(I - C)Z_K + CZ_{L_1}$, which is of bounded type I, so therefore L_2 itself is a bounded type I group. Now $E([L_2], \alpha) \geqq D$, and if we take $\delta < \epsilon/2n(n+1)$, it follows that $\lambda(E([L_2], \alpha)) > 1 - \epsilon$. By Lemma 4.5, for an appropriate integer n, there exists a type I_n subgroup L of $[G]$ such that $[L_2] \subset [L]$. Automatically, $\lambda(E[L], \alpha)) > 1 - \epsilon$, and the lemma is proved.

As we have noted in Lemma 4.3, any finite freely acting group K has an

abelian basis of the form $[kP \mid k \in K]$, and conversely, if P is any projection such that the kP are mutually orthogonal and $\sum kP = I$, then the kP form an abelian basis for K. By a *basis algebra* $\mathcal{B}$ for K we mean the finite K-invariant boolean algebra generated by an abelian basis of the form kP $(k \in K)$. By a generator of such an algebra we mean any one of its atoms, that is, any kP. In the following we speak of *couples* $(K, \mathcal{B})$, where K is understood to be a finite freely acting subgroup of $[G]$ and $\mathcal{B}$ a basis algebra for K.

Definition 6.1. A set of couples $(K_i, \mathcal{B}_i)$ $(1 \leqq i \leqq n)$ is said to be *mutually independent* if, for each pair i, j with $i \neq j$, K_i lies in the centralizer of K_j and $\mathcal{B}_i$ is contained in the fixed algebra Z_j of K_j.

It is clear, of course, that the $(K_i, \mathcal{B}_i)$ are mutually independent if and only if they are pairwise independent.

LEMMA 6.2. *If the couples $(K_i, \mathcal{B}_i)$ $(1 \leqq i \leqq n)$ are mutually independent, then* 1) *the group K generated by the K_i is freely acting and algebraically is a direct product $K_1 \times K_2 \times \cdots \times K_n$,* 2) $E_{Z_1 \cap \cdots \cap Z_n} = E_{Z_1} E_{Z_2} \cdots E_{Z_n}$, *and* 3) *if $Q_i \in \mathcal{B}_i$, then*

$$\lambda(Q_1 \cdots Q_n) = \lambda(Q_1)\lambda(Q_2) \cdots \lambda(Q_n).$$

Proof. (1) Say $k_1 k_2 \cdots k_n$ leaves a non-zero projection P absolutely fixed $(k_i \in K_i)$. For each i, P dominates a non-zero projection of the form CP_i (P_i a generator of $\mathcal{B}_i$, C in Z_i), and because $\mathcal{B}_i \subset Z_j$ $(j \neq i)$, we have $CP_i = (k_1 \cdots k_n)(CP_i) = (k_1 \cdots k_n)(C) k_i(P_i)$. This implies $k_i = e$, for otherwise $CP_i = CP_i k_i P_i = 0$, a contradiction. Therefore, $k_1 = \cdots = k_n = e$, and K is freely acting. A fortiori, $k_1 k_2 \cdots k_n = e$ entails $k_1 = \cdots = k_n = e$, and it follows that K is a direct product $K_1 \times \cdots \times K_n$.

(2) Each k in K_i implements an automorphism of Z_j $(j \neq i)$, since by assumption k lies in the centralizer of K_j. By (2.6), therefore, $kE_{Z_j} = E_{Z_j} k$, and we have

$$kE_{Z_1} \cdots E_{Z_n}(P) = E_{Z_1} \cdots E_{Z_{j-1}} k E_{Z_j} \cdots E_{Z_n}(P) = E_{Z_1} \cdots E_{Z_n}(P).$$

It follows that $E_{Z_1} \cdots E_{Z_n}(P)$ lies in the fixed algebra $Z = Z_1 \cap \cdots \cap Z_n$ of K. Plainly $\lambda[C(E_{Z_1} \cdots E_{Z_n}(P))] = \lambda(CP)$, for each C in Z and P in M, and by the uniqueness of E_Z (remark following (2.1)), we have $E_Z = E_{Z_1} \cdots E_{Z_n}$, as asserted. The statement (3) of the lemma follows readily from the fact that Q_i in $\mathcal{B}_i$ entails $E_{Z_j}(Q_i) = Q_i$ $(j \neq i)$ and $E_{Z_i}(Q_i) = \lambda(Q_i)$.

LEMMA 6.3. *Assume G approximately finite. Let $(K, \mathcal{B}_K)$ be a given couple, and let α be an arbitrary element of $[G]$. Then, for each $\epsilon > 0$, there exists a couple $(L, \mathcal{B}_L)$ independent of $(K, \mathcal{B}_K)$, where L is a cyclic group with order a power of two, and $\lambda(E([K \times L], \alpha)) > 1 - \epsilon$.*

Proof. Choose $\delta > 0$ (to be specified later) and apply Lemma 6.1: there exists a type I_m subgroup L_1 of $[G]$ such that $K \subset [L_1]$ and $\lambda(E([L_1], \alpha)) > 1 - \delta$. If $n =$ order K, then n divides m and we can write $m = nt$. Choose an integer a such that $t/2^a < \delta$, and then choose an integer b such that $b/2^a \leqq 1/t < (b+1)/2^a$. One has $1 \geqq bt/2^a > 1 - t/2^a > 1 - \delta$. The fixed algebra Z of G is of type II in Z_{L_1}, and so by Maharam's lemma, there exists a projection C in Z_{L_1} such that $E_Z(C) = bt/2^a$. Let P be a generator of $\mathcal{B}_K$, so $E_{Z_K}(P) = 1/n$, and $E_Z(CP) = E_Z(E_{Z_K}(CP)) = E_Z(CE_{Z_K}(P)) = bt/n2^a$. Now $[L_1]_C$ is a type I_{nt} subgroup of $[G]_C$ on CM. By Lemma 4.5 (first part of proof), we can find a subgroup L_2 of $[G]_C$ on CM of type I_{nbt} such that $[L_1]_C \subset [L_2]$. Now, we claim, CP can be partitioned $CP = P_0 + \cdots + P_{bt-1}$, where the P_i are part of an abelian basis for L_2. In fact, the Z_{L_2}-carrier of CP is C, so CP dominates an abelian projection P_0 of L_2 with Z_{L_2}-carrier C. One has $E_{Z_{L_2}}(PC - P_0) = (1/n - 1/nbt)C$, so $PC - P_0$ is either 0 or again has Z_{L_2}-carrier C. In the latter case, $PC - P_0$ dominates an abelian projection P_1 of L_2 with Z_{L_2}-carrier C. Iteration of argument will lead to the ascribed partition. By the familiar method, choose a ρ in $[L_2]$ such that $\rho(P_i) = P_{i+1}$ (indices mod bt), $\rho^{bt} =$ identity, and $\rho =$ identity off PC.

Turning to $(I - C)$, we have $E_Z(P(I - C)) = (2^a - bt)/n2^a$, and by Maharam's lemma, we can partition $P(I - C) = Q_0 + \cdots + Q_{2^a - bt - 1}$ as a sum of mutually orthogonal projections each with expectation $1/n2^a$ relative to Z. Choose a β in $[G]$ which sends Q_i into Q_{i+1} (indices mod $2^a - bt$) and has order $2^a - bt$. Next, choose a γ in $[G]$ such that $\gamma(P_{bt-1}) = Q_0$, $\gamma^2 =$ identity. Define τ in $[G]$ as follows: first, set $\tau_1 = \rho$ on P_i $(i < bt - 1)$, $\tau_1 = \gamma$ on P_{bt-1}, $\tau_1 = \beta$ on Q_i $(i < 2^a - bt - 1)$, and $\tau_1 = \rho\gamma\beta$ on $Q_{2^a - bt - 1}$; and then define $\tau(Q) = k\tau_1 k^{-1}(Q)$ for $Q \leqq kP$ (k in K). It follows readily that τ generates a freely acting cyclic group L on M of order 2^a, that τ commutes with K, and that $\mathcal{B}_K \subset Z_L$. Take $\sum_{k \in K} kP_0$ as the generator of a basis algebra $\mathcal{B}_L$ of L. Then $\mathcal{B}_L \subset Z_K$, and $(K, \mathcal{B}_K)$, $(L, \mathcal{B}_L)$ are independent couples. Since the automorphism ρ agrees on $P_0 + \cdots + P_{bt-2}$ with τ, on P_{bt-1} with τ^{1-bt}, and is the identity elsewhere, we have $\rho \in [L]$. Therefore, the group K_0 on CM generated by ρ (on CM) and $[K]_C$ lies in $[K \times L]_C$.

Also $K_0 \subset [L_2]$, and that equality $[K_0]=[L_2]$ holds follows from the readily verified fact that R in Z_{K_0} entails R in Z_{L_2}. Therefore, $[L_2]=[K_0] \subset [K \times L]_C$. Already, $[L_1]_C \subset [L_2]$, and we recall that $\lambda(E([L_1],\alpha)) > 1-\delta$, namely, $[L_1]$ contains an α_1 which agrees with α on a projection of measure $>1-\delta$. The automorphism α_2 defined to be α_1 on C and the identity elsewhere therefore agrees with α on a projection of measure $>1-2\delta$, and $\alpha_2 \in [K \times L]$. We have $\lambda(E([K\times L],\alpha)) > 1-2\delta$. Take $\delta < \epsilon/2$, and the lemma follows.

LEMMA 6.4. *Let $(K,\mathcal{B})$ be a couple, with cyclic of order 2^n. Then there exist mutually independent couples $(K_i,\mathcal{B}_i)$ such that K_i has order 2, $[K]=[K_1\times\cdots\times K_n]$, $\mathcal{B}$ is generated by the $\mathcal{B}_i$, and any couple $(L,\mathcal{C})$ independent of $(K,\mathcal{B})$ is independent of each $(K_i,\mathcal{B}_i)$.*

Proof. Set $\Lambda=(0,1,\cdots,2^n-1)$. For $1\leqq m\leqq n$, define S_m as $[i \text{ in } \Lambda \mid (j-1)2^{n-m}\leqq i < j2^{n-m}, \text{ for some odd integer } j]$. Let P be a generator of $\mathcal{B}$ and α a generator of K. Define $R_m=\sum_{i\in S_m}\alpha^i P$, and define $\alpha_m=\alpha^{2^{m-n}}$ on R_m, $\alpha_m=\alpha^{-2^{m-n}}$ on $I-R_m$. Because $S_m\pm 2^{n-m}=\Lambda-S_m$ (mod 2^n), we have $\alpha_m(R_m)=I-R_m$, $\alpha_m{}^2=$ identity. Therefore α_m is an automorphism in $[K]$. Moreover, if $p\neq m$, then $S_m\pm 2^{n-p}=S_m$ (mod 2^n), whence $\alpha_p(R_m)=R_m$. Now for any Q and $p\neq m$,

$$\begin{aligned}\alpha_m\alpha_p Q &= \alpha^{2^{n-m}+2^{n-p}}(Q)(I-R_m)(I-R_p)+\alpha^{2^{n-m}-2^{n-p}}(Q)R_p(I-R_m)\\ &\quad+\alpha^{-2^{n-m}+2^{n-p}}(Q)(I-R_p)R_m+\alpha^{-2^{n-m}-2^{n-p}}(Q)R_mR_p,\end{aligned}$$

which is symmetric in p and m. Therefore, α_p and α_m commute. If we set $K_m=\{e,\alpha_m\}$ and $\mathcal{B}_m=\{R_m, I-R_m\}$, it follows that the couples $(K_i,\mathcal{B}_i)$ are mutually independent. Now if G_1 and G_2 are type I_s groups and if $G_1\subset[G_2]$, then $[G_1]=[G_2]$. Applying this fact here, we have $[K]=[K_1\times\cdots\times K_n]$. The boolean algebra $\mathcal{B}_0$ generated by the $\mathcal{B}_i$ is K_i-invariant and the projection $P=R_1\cdots R_m$ is an atom in $\mathcal{B}_0$. Because $K_1\times\cdots\times K_n$ is freely acting and P is abelian for $[K]=[K_1\times\cdots\times K_n]$, it follows that P is orthogonalized by $K_1\times\cdots\times K_n$ (Lemma 4.1). Therefore $I=\sum_{k\in K_1\times\cdots\times K_n} kP$, all kP lie in $\mathcal{B}_0$, and accordingly, $\mathcal{B}_0$ is a basis algebra for $K_1\times\cdots\times K_n$. But $\mathcal{B}_0$ is a subalgebra of $\mathcal{B}$ having the same number of atoms, whence $\mathcal{B}_0=\mathcal{B}$. Let $(L,\mathcal{C})$ be a couple independent of $(K,\mathcal{B})$. For each i, we have $\mathcal{C}\subset Z_K\subset Z_{K_i}$, and $\mathcal{B}_i\subset\mathcal{B}\subset Z_L$. Finally, if $\gamma\in L$, then $\gamma R_m=R_m$, and for any Q,

$$\begin{aligned}(\gamma\alpha_m)(Q) &= \gamma[\alpha^{2^{n-m}}(Q)(I-R_m)+\alpha^{-2^{n-m}}(Q)R_m]\\ &= \alpha^{2^{n-m}}(\gamma Q)(I-R_m)+\alpha^{-2^{n-m}}(\gamma Q)R_m=(\alpha_m\gamma)(Q).\end{aligned}$$

Therefore, L lies in the centralizer of K_i. It follows that $(L, \mathcal{C})$ is independent of each $(K_i, \mathcal{B}_i)$, proving the lemma.

In the following, we call an automorphism group G countably generated if it is equivalent to a countable automorphism group. [If G is freely acting and countably generated, then it is easy to see that G must be countable.]

THEOREM 3. *Let G be a countably generated type II group of MP automorphisms of (M, λ). In order that G be approximately finite, it is necessary and sufficient that G be equivalent to a freely acting automorphism group $K = \prod_{n=1}^{\infty} K_n$, K being the restricted direct product of a countably infinite set of freely acting groups K_n each of order two.*

Proof. As noted in Section 5, sufficiency is clear. To prove necessity, we can suppose that the approximately finite group G is countably infinite. Let α_n be a sequence such that each $\alpha_n \in G$ and each g in $G = \alpha_n$, for infinitely many n. By repeated application of Lemma 6.3, we can construct a sequence of couples $(L_n, \mathcal{B}_n)$ with the following properties: $L_n \subset [G]$, order $L_n = 2^{r_n}$, $(L_n, \mathcal{B}_n)$ is independent of $(L_i, \mathcal{B}_i)$, for $1 \leqq i < n$, and $\lambda(E([L_1 \times \cdots \times L_n], \alpha_n)) < 1/n$. For each $(L_n, \mathcal{B}_n)$, select couples $(L_i^{(n)}, \mathcal{B}_i^{(n)})$ $(1 \leqq i \leqq r_n)$ satisfying the conclusion of Lemma 6.4. Denote by $(K_1, \mathcal{C}_1), (K_2, \mathcal{C}_2), \cdots$ the sequence $(L_1^{(1)}, \mathcal{B}_1^{(1)}), \cdots, (L_{r_1}^{(1)}, \mathcal{B}_{r_1}^{(1)})$, $(L_1^{(2)}, \mathcal{B}_1^{(2)}), \cdots, (L_{r_2}^{(2)}, \mathcal{B}_{r_2}^{(2)})$, $(L_1^{(3)}, \mathcal{B}_1^{(3)})$, etc. The $(K_i, \mathcal{C}_i)$ are pairwise independent. Therefore the group K generated by the K_i is freely acting and is the restricted direct product $K = \prod_{i=1}^{\infty} K_i$. For each n, $\lambda(E([K], \alpha_n)) < 1/n$, and therefore, for each g in G, $\lambda(E([K], g)) = 0$, giving $[G] \subset [K]$. Equality $[G] = [K]$ follows by construction of K, and the theorem is proved.

A fortiori, if the countably generated type II group G is approximately finite, then G is equivalent to a freely acting group. Is the same true when G is not assumed approximately finite? This question is not settled.

LEMMA 6.5. *Let G be a type II group with fixed algebra Z. Let $(K, \mathcal{B}_K)$ be a given couple, with $K \subset [G]$ and order $K = 2^m$, and let P be a projection in M. Then, for each $\epsilon > 0$, there exists a couple $(L, \mathcal{B}_L)$ independent of $(K, \mathcal{B}_K)$, with $L \subset [G]$ and order L a power of two, such that, if $\mathcal{B}$ denotes the boolean algebra generated by $\mathcal{B}_L$, $\mathcal{B}_K$ and Z_P, then $\inf_{C \in \mathcal{B}} \lambda(P \Delta C) < \epsilon$.*

Proof. Let R be a generator for $\mathcal{B}_K$, and let $\mathcal{C}$ denote the finite K-invariant boolean algebra generated by $\mathcal{B}_K$ and the translates kP $(k \in K)$ of P. As a member of $\mathcal{C}$, R is a sum of atoms $R = R_1 + \cdots + R_s$ of $\mathcal{C}$,

and any atom of $\mathcal{B}$ is a translate by K of one of these R_i. Select a $\delta > 0$ (to be specified later). Choose mutually orthogonal projections $D_1, \cdots, D_t$ in Z with $\sum_i D_i = I$ and scalars $a_{ij} \geqq 0$ $(1 \leqq i \leqq s, 1 \leqq j \leqq t)$ such that

$$E_Z(R_i) - \delta/2 \leqq \sum_{j=1}^{t} a_{ij} D_j \leqq E_Z(R_i) \qquad (1 \leqq i \leqq s). \tag{6.1}$$

(That this choice is possible becomes clear if one considers the functional representation $C(\Gamma_Z)$ of Z, Γ_Z being the spectrum of Z.) Moreover, it is clear that we can find a sufficiently large integer p such that, if $\rho = 2^{-(m+p)}$ and n_{ij} = the largest non-negative integer satisfying $n_{ij}\rho \leqq a_{ij}$, then

$$E_Z(R_i) - \delta \leqq \sum_{j=1}^{t} n_{ij}\rho D_j \leqq E_Z(R_i) \qquad (1 \leqq i \leqq s). \tag{6.2}$$

Now fix the pair (i, j) with $n_{ij} \neq 0$, and applying Maharam's lemma, choose mutually orthogonal projections $R_{ik}^{(j)} \leqq R_i D_j$ such that $E_Z(R_{ik}^{(j)}) = \rho D_j$ $(1 \leqq k \leqq n_{ij})$. Set $R_{i0}^{(j)} = R_i D_j - \sum_k R_{ik}^{(j)}$ $(n_{ij} \neq 0)$ and $R_{i0}^{(j)} = R_j D_j$ $(n_{ij} = 0)$. From (6.2), we infer that

$$E_Z(R_{i0}^{(j)}) < \delta D_j \qquad (1 \leqq j \leqq t). \tag{6.3}$$

Now $E_Z(D_j R) = D_j E_Z(R) = D_j/2^m = 2^p \rho D_j$, and $D_j R = \sum_{i=1}^{s} D_j R_i = \sum_{i=1}^{s} \sum_{k=0}^{n_{ij}} R_{ik}^{(j)}$, where (by (6.3)) $E_Z(\sum_{i=1}^{s} R_{i0}^{(j)}) < s\delta D_j$. Therefore, $D_j R$ is partitioned into a sum of $N_j = \sum_{i=1}^{s} n_{ij}$ mutually orthogonal projections $R_{ik}^{(j)}$ $(k > 0)$, each with expectation ρD_j relative to Z, and the complement of this sum in $D_j R$ has Z-expectation $(2^p - N_j)\rho D_j < s\delta D_j$. Denote these $R_{ik}^{(j)}$ $(k > 0)$ by $S_1^{(j)}, \cdots, S_N^{(j)}$, and again by Maharam's lemma, choose mutually orthogonal projections $S_{N_j+1}^{(j)}, \cdots, S_{2^p}^{(j)}$, each with expectation ρD_j relative to Z, such that $D_j R = \sum_{k=1}^{2^p} S_k^{(j)}$. Let $S_k = \sum_{j=1}^{t} S_k^{(j)}$ $(1 \leqq k \leqq 2^p)$. Then $R = \sum S_k$ and $E_Z(S_k) = \rho$. Choose an $\alpha \in [G]$ such that $\alpha(S_k) = S_{k+1}$, $(1 \leqq k \leqq 2^p - 1)$, $\alpha(S_{2^p}) = S_1$, α^{2^p} = identity, α = identity off R. Next, define β in $[G]$ as follows: $\beta(Q) = k\alpha k^{-1}(Q)$ when $Q \leqq kR$ $(k \in K)$. This automorphism β commutes with each k in K and generates a freely acting cyclic group L of order 2^p. Let $Q = \sum_{k \in K} kS_1$. Then each $\beta^i Q \in Z_K$, and

$$\sum_{i=1}^{2^p} \beta^i Q = \sum_{k \in K} k[\sum_{i=1}^{2^p} \beta^i S_1] = \sum_{k \in K} kR = I.$$

Thus, the $\beta^i Q$ generate a basis algebra $\mathcal{B}_L$ for L, and $\mathcal{B}_L \subset Z_K$. By construction, $\mathcal{B}_K \subset Z_L$. It follows that $(L, \mathcal{B}_L)$ and $(K, \mathcal{B}_K)$ are independent couples, and L has order a power of two.

We return to the given P in $\mathscr{C}$. This P has the form $P = \sum_{k \in K} kE_K$, where each $E_k \leqq R$ and is 0 or a sum of R_i's. Denote by F_k the sum of all projections of the form $R_{ik}^{(j)}$ $(k > 0)$ which are dominated by E_k. Each of these $R_{ik}^{(j)}$ lies in the boolean algebra $\mathscr{B}$ generated by $\mathscr{B}_K$, $\mathscr{B}_L$ and Z_P: for $QR = S_1$, so all S_k lie in the algebra generated by $\mathscr{B}_K$ and $\mathscr{B}_L$, and the $R_{ik}^{(j)}$ are obtained as slices of the S_k by elements of Z_P. For any $R_i \leqq E_k$, we have $E_Z(R_i - R_iF_k) < \delta$ (by (6.3)), so $E_Z(E_k - F_k) < s\delta$, and $E_Z(P - \sum_{k \in K} kF_k) < 2^m s\delta$. But $\sum_{k \in K} kF_k \in \mathscr{B}$. If we take $\delta < \epsilon/s2^m$ (and note that m and s depend only on K and P), the lemma follows.

We say that (M, λ) is countably generated over a hyperstonian subalgebra Z if there exists a sequence P_n in M_P such that the boolean algebra generated by the P_n and Z_P is dense in M_P relative to the metric $\lambda(P \Delta Q)$. [This is equivalent to the following: there exists a sequence A_n in M such that the *-algebra generated by the A_n and Z is dense in M relative to the norm $\lambda[(A - B)(A - B)^*]^{\frac{1}{2}}$.]

THEOREM 4. *Let G be a type II group of MP automorphisms of (M, λ) with fixed algebra Z. Assume that (M, λ) is countably generated over Z. Then $[G]$ contains an approximately finite subgroup K with the same fixed algebra Z, and which is maximal among such subgroups of $[G]$.*

Proof. Let P_n be a sequence of projections in M which generate M over Z in the above sense. Let Q_n be a sequence of projections such that each Q_n lies in the sequence P_n and each P_n occurs infinitely often in the sequence Q_n. Repeated application of Lemma 6.5 yields a sequence of pairwise independent couples $(L_n, \mathscr{B}_n)$ with this property: for each n, the boolean algebra generated by $\mathscr{B}_1, \cdots, \mathscr{B}_n$ and Z_P contains a projection R_n such that $\lambda(R_n \Delta Q_n) < 1/n$. Let L be the freely acting approximately finite group $L = \prod_{n=1}^{\infty} L_n$, and let $\mathscr{B}$ be the boolean algebra generated by the $\mathscr{B}_n$. By construction, the boolean algebra $\mathscr{C}$ generated by $\mathscr{B}$ and Z_P is dense in M_P in the $\lambda(P \Delta Q)$ metric.

We claim, $Z = Z_L$, where Z_L is the fixed algebra of L. Take $P \in Z_L$. For each $\epsilon > 0$, there exist projections P_i in $\mathscr{B}$ and C_i in Z such that $\lambda(P \Delta \sum P_i C_i) < \epsilon$. Now any projection R in $\mathscr{B}$ (or for that matter, in the λ-closure $\bar{\mathscr{B}}$ of $\mathscr{B}$) is independent of Z_L, that is, has constant expectation relative to Z_L: this is obvious for projections in the boolean algebra generated by $\mathscr{B}_1, \cdots, \mathscr{B}_n$, since atoms in this algebra are abelian relative to $L_1 \times \cdots \times L_n$; and for any element R in $\bar{\mathscr{B}}$, we can find a sequence R_n such that $\lim_n \lambda(R \Delta R_n) = 0$ and R_n lies in the boolean algebra generated by

$\mathcal{B}_1, \cdots, \mathcal{B}_n$; $E_{Z_L}(R_n)$ is a constant c_n, so that $\lambda(R_n) = \lambda(E_{Z_L}(R_n)) = c_n$, and (using (2.7)) $E_{Z_L}(R) = \lim_n E_{Z_L}(R_n) = \lim \lambda(R_n) = \lambda(R)$, proving that R is independent of Z_L. Therefore, $E_{Z_L}(\sum P_i C_i) = \sum \lambda(P_i) C_i$ lies in Z, from which it follows that $P = E_{Z_L}(P) \in Z$. This shows that $Z_L \subset Z$. But since $L \subset [G]$, we must have $Z \subset Z_L$. Therefore $Z = Z_L$.

We have established the existence of approximately finite subgroups of $[G]$ having the same fixed algebra as G. To conclude, we wish to construct an approximately finite subgroup K of $[G]$ having fixed algebra Z and which is not contained in any larger approximately finite subgroup of $[G]$. The existence of K follows readily from Zorn's lemma. In fact, order full approximately finite subgroups of $[G]$ containing L by inclusion, and let L_a $(a \in A)$ be a maximal linearly ordered subset. Let $K = [\bigcup_a L_a]$. K will of course have fixed algebra Z, and that K is approximately finite follows easily from the fact that, given α in K, there exists a finite set of indices $a_1, \cdots, a_n$ in A and elements g_i in L_{a_i} such that $\lambda(\bigcup_i F(\alpha, g_i)) > 1 - \epsilon$, for a preassigned $\epsilon > 0$; by linear order, these g_i will lie in some one L_a, and therefore $\lambda(E([L_a], \alpha)) > 1 - \epsilon$; application of the assumed approximate finiteness of the L_a then completes the proof.

The maximal approximately finite subgroup K of $[G]$ constructed in Theorem 4 will not in general be unique. In fact, it is not hard to show that, if $[G]$ contains precisely one maximal approximately finite subgroup, then G is already approximately finite and that subgroup coincides with $[G]$.

7. Weak equivalence of groups.

Definition 7.1. Let (M, λ) and (M', λ') be abstract non-atomic hyperstonian measure spaces. Let G (respectively, G') be a group of MP automorphisms of (M, λ) (respectively, (M', λ')). G and G' are called *weakly equivalent* if there exists an isomorphism ($=$ *-isomorphism) φ of M on M' such that the transplant $\varphi^{-1}G'\varphi$ of G' is equivalent to G.

We do not require φ to be measure preserving, though it is clear that each $\varphi^{-1}g'\varphi$ $(g' \in G')$ will be a measure preserving automorphism of (M, λ), since any element of $[G]$ is automatically MP. If φ is not MP, then one can introduce a new measure λ_1 on M, equivalent to λ, and relative to which φ is MP and G remains an MP group; this fact is contained in the proof of the theorem to follow.

THEOREM 5. *Let G and G' be approximately finite type II group of MP automorphism of (M, λ) and (M', λ'), with fixed algebras Z and Z'. Assume that G and G' are countably generated, and that M (respectively M')*

is countably generated over Z (respectively Z'). Then in order that G and G' be weakly equivalent, it is necessary and sufficient that there exist an algebraic isomorphism θ of Z on Z'.

Proof. Necessity is trivial: if G and G' are weakly equivalent via an isomorphism φ, then the fixed algebra of $\varphi^{-1}G'\varphi$ is $\varphi^{-1}Z'$, so automatically $\varphi Z = Z'$. We turn to sufficiency. The main step here comes from iterated application of Lemmas 6.3-6.5, as in Theorem 3 and 4. One constructs a sequence of couples $(K_n, \mathcal{B}_n)$ such that, first, each K_a is freely acting of order two and G is equivalent to the freely-acting product group $\prod_n K_n$, and second, if $\mathcal{B}$ is the boolean algebra generated by the $\mathcal{B}_n$ and $\mathcal{C}$, the boolean algebra generated by $\mathcal{B}$ and Z_P, then $\mathcal{C}$ is dense in M_P in the λ-metric. (The procedure in the construction of the couples $(K_n, \mathcal{B}_n)$ is to approximate alternately to elements of a generating set for G and a generating set for M over Z.) This construction applied to (M', λ') yields a sequence $(K'_n, \mathcal{B}'_n)$ with the analogous properties.

Let $K = \prod_n K_n$, $K' = \prod_n K'_n$. It is evident that there exists an isomorphism $g \to g'$ of K on K' which sends K_n (qua subgroup of K) on K'_n, for each n. By the same token, it is easy to see that there exists a boolean isomorphism φ of $\mathcal{B}$ on $\mathcal{B}'$ such that

$$\varphi(kP) = k'\varphi(P), \qquad \theta(E_Z(P)) = E_{Z'}(\varphi(P)), \tag{7.1}$$

for all $k \in K$, $P \in \mathcal{B}$; for recall that $\mathcal{B}$ is the union of an increasing sequence of boolean algebras (these generated by the $\mathcal{B}_i$, $1 \leq i \leq n$), each of whose atoms is an abelian projection for $K_1 \times \cdots \times K_n$. Now $\mathcal{C}$ consists of projections of the form $P = \sum_{i=1}^{r} P_i C_i$ $(P_i \in \mathcal{B}, C_i \in Z_P)$, in the representation of which we can assume the C_i are mutually orthogonal. If $P = \sum_{j=1}^{s} Q_j D_j$ is another such representation of P, then $P_j C_i D_j = Q_j C_i D_j$ for all i and j. From this it follows that $P_i = Q_j$ if $C_i D_j \neq 0$: in fact, if $\mathcal{B}$ contains a non-zero projection R such that $RP_i = R$ and $RQ_j = 0$, then $RC_i D_j = 0$, so $E_Z(R) C_i D_j = 0$, so $C_i D_j = 0$, because $E_Z(R)$ is a constant. Therefore, $\varphi(P_i) = \varphi(Q_j)$ if $\theta(C_i)\theta(D_j) \neq 0$, and $\varphi(P_i)\theta(C_i D_j) = \varphi(Q_j)\theta(C_i D_j)$ holds in all cases. This show that $\sum \varphi(P_i)\theta(C_i) = \sum \varphi(Q_j)\theta(D_j)$. If we now define $\varphi(P) = \sum \varphi(P_i)\theta(C_i)$ (for C_i mutually orthogonal), then this definition is single-valued, and φ is plainly a boolean isomorphism of $\mathcal{C}$ on $\mathcal{C}'$. It is clear, moreover, that the formula (7.1) now holds for all P in $\mathcal{C}$. Note that this formula shows that $P \in Z$ if and only if $\varphi(P) \in Z'$, and that $\theta(P) = \varphi(P)$, for P in Z.

We now introduce an equivalent measure λ_1 on M relative to which φ is MP. First of all, for A in Z, set $\lambda_0(A) = \lambda'(\theta(A))$. Then λ_0 is a faithful measure on Z which is normal, this because θ and λ' are normal. Next, for A in M, define $\lambda_1(A) = \lambda_0(E_Z(A))$. Clearly λ_1 is a measure. It is faithful, for if $A \geqq 0$ and $\lambda_1(A) = 0$, then $\lambda_0(E_Z(A)) = 0$, so $E_Z(A) = 0$, $A \doteq 0$. It is normal: if the A_a are bounded and SA, then

$$\begin{aligned}\mathrm{LUB}_a \lambda_1(A_a) &= \mathrm{LUB}_a \lambda_0(E_Z(A_a)) = \lambda_0(\mathrm{LUB}_a E_Z(A_a)) \\ &= \lambda_0(E_Z(\mathrm{LUB}_a A_a)) = \lambda_1(\mathrm{LUB}_a A_a).\end{aligned}$$

For any α in $[K]$, $\lambda_1(\alpha A) = \lambda_0(E_Z(\alpha A)) = \lambda_0(E_Z(A)) = \lambda_1(A)$, so $[K]$ remains an MP group. Now $\lambda_1(P) = 0$ if and only if $P = 0$ if and only if $\lambda(P) = 0$, for any projection P, so λ_1 is equivalent to λ. Finally, φ is MP relative to λ_1: $\lambda_1(P) = \lambda_0(E_Z(P)) = \lambda'(\theta(E_Z(P)) = \lambda'(E_Z(P)) = \lambda'(\varphi(P))$. It follows that (M, λ_1) is hyperstonian, and that φ is an isometry of $\mathcal{B}$ on $\mathcal{B}'$ relative to the λ_1 and λ' metrics. Therefore, φ can be extended uniquely to an isomorphism of M on M', the conditions (7.1) now being valid for all P in M.

We have $\varphi^{-1}k'\varphi = k$ for each $k \in K$, so $\varphi^{-1}K'\varphi$ is trivially equivalent to K. By construction, K is equivalent to G, K' to G', and by the transitivity of equivalence, we see that $\varphi^{-1}G'\varphi$ is equivalent to G. This proves the theorem.

If G and G' are type I_n groups on M and M' with fixed algebras Z and Z', and if there exists an isomorphism θ of Z on Z', then θ extends to an isomorphism φ of M on M' such that $\varphi^{-1}G'\varphi = G$: in fact, we can assume (up to equivalence) that G and G' are freely acting cyclic groups of order n, with generator α and β, and with abelian bases $\alpha^i(P)$ and $\beta^i(Q)$; this done, define $\varphi(\sum_i D_i\alpha^i P) = \sum_i \theta(D_i)\beta^i Q$ $(D_i \in Z)$ to obtain the desired isomorphism φ. Now given any group G with fixed algebra Z, there exist uniquely determined projection $C_\infty, C_1, C_2, \cdots$ in Z such that G_{C_i} is of type I_i (i finite) or II $(i = \infty)$. Under a weak equivalence of G with a group G', one will have $\varphi(C_n) = C'_n$, where the C'_n determine the type summands of G'. It follows easily from this discussion that Theorem 5 remains valid for groups G and G' not necessarily of type II if one adjoins the condition that $\theta(C_n) = C'_n$, for all n.

8. The existence of non-approximately finite groups. The detection of non-approximately finite groups in this presentation, as in the Murray-von Neumann construction, hinges on the derivation of necessary conditions which cannot be realized for certain groups, this by virtue of their algebraic (opposed to action) characteristics. The necessary conditions developed here

(Lemma 8.1), apparently unlike the "property Γ" of Murray-von Neumann, also turn out to be sufficient conditions, and the further development of the theory profits from this circumstance.

LEMMA 8.1. *Let K be a countable freely acting group of MP automorphisms of M. Assume that K is approximately finite. Then for any finite subset $x_1,\cdots,x_n$ of K and each $\epsilon>0$, there exists a function $x\to E_x$ from K to M_P with the following properties:* (1) $E_xE_{xy}=E_xx(E_y)$ *and* $E_e=I$; (2) $\lambda(\prod_{i=1}^{n}E_{x_i})>1-\epsilon$; (3) $\sum_x E_x$ *is bounded.*

Proof. By Theorem 3, K is equivalent to a freely acting group G which is algebraically the union of an increasing sequence of finite subgroups. Given x_i in K $(1\leqq i\leqq n)$ and $\epsilon>0$, it is clear that we can find a finite subgroup S of G such that $\lambda\,(\prod_{i=1}^{n}E([S],x_i))>1-\epsilon$. Let $E_x=E([S],x)$. We will show that this function has the ascribed properties.

By Lemma 3.1, each x in K has a representation

$$x(P)=\sum_{g\in G}Q(g,x)g(P),\tag{8.1}$$

where for each x, the sets $Q(g,x)$, respectively, $g^{-1}Q(g,x)$, are mutually orthogonal and have LUB I. Because G is freely acting, the coefficient projections $Q(g,x)$ in (8.1) are uniquely determined; and because K is freely acting, $Q(g,x)Q(g,y)=0$ if $x\neq y$. Computing $x(y(P))$ from (8.1) and comparing terms with $(xy)(P)$, we get

$$Q(g,xy)=\sum_{h\in G}Q(h,x)h[Q(h^{-1}g,y)].\tag{8.2}$$

Now (8.1) also shows that $F(x,g)=g^{-1}Q(x,g)$. But $E_x=\mathrm{LUB}_{g\in S}\,gF(x,g)$, so that

$$E_x=\sum_{g\in S}Q(g,x).\tag{8.3}$$

From this, we obtain $\sum_{x\in K}E_x=\sum_{g\in S}[\sum_{x\in K}Q(g,x)]\leqq$ order S. This establishes condition (3) of the lemma. To verify condition (1), we use (8.2) to compute $E_{xy}=\sum_{g\in S}\sum_{h\in G}Q(h,x)h[Q(h^{-1}g,y)]$, so that

$$E_xE_{xy}=\sum_{g,h\in S}Q(h,x)h[Q(h^{-1}g,y)];$$

further,

$$xE_y=\sum_{h\in G}Q(h,x)h[\sum_{g\in S}Q(g,y)]=\sum_{h\in G}\sum_{g\in S}Q(h,x)h[Q(g,y)],$$

so

$$E_xxE_y=\sum_{h,g\in S}Q(h,x)h[Q(g,y)]=\sum_{h,g\in S}Q(h,x)h[Q(h^{-1}g,y)]=E_xE_{xy}.$$

Obviously $E_e=I$, and the lemma is proved.

PROPOSITION 8.1. *Let K be a countable discrete group. Suppose that K contains a subset F and elements x, y, z such that 1) $F \cup xF = K$, 2) $yF \cap zF = \phi$, and 3) $yF \cup zF \subset xF$. Then, in any faithful representation as a freely acting group of MP automorphisms of a non-atomic hyperstonian measure space (M, λ), K is non-approximately finite.*

Proof. We assume that K has a freely-acting faithful approximately finite representation on (M, λ) and will arrive at a contradiction. Take $0 < \epsilon < 1/5$. Let E_x be the function on K to M_P with the properties (1)-(3) of Lemma 8.1 for the subset x, y, z and this ϵ: one has $\lambda(E_xE_yE_z) > 1 - \epsilon$, the function $T = \sum_{u \in K} E_u$ is bounded, and $E_uE_{uv} = E_u uE_v$, $E_e = I$. Let $A = \sum_{u \in F} E_u$. By conditions (2) and (3) in the proposition,

$$(8.4) \qquad \sum_{u \in F} (E_{yu} + E_{zu}) = \sum_{u \in yF} E_u + \sum_{u \in zF} E_u \leqq \sum_{u \in xF} E_u.$$

Multiply both sides of (8.4) by $E_xE_yE_z$ and use the relations $E_yE_{yu} = E_y yE_u$, etc. Then

$$(8.5) \qquad E_xE_yE_z[yA + zA] \leqq E_xE_yE_z x(A).$$

Now $E_vT = \sum_u E_vE_u = \sum_u E_vE_{vu} = \sum_u E_v vE_u = E_v v(T)$. T^{-1} exists, since $T \geqq I$, and we obtain

$$(8.6) \qquad E_vT^{-1} = E_v v(T^{-1}).$$

Let $B = AT^{-1}$, and multiply both sides of (8.5) by T^{-1} to obtain

$$(8.7) \qquad E_xE_yE_z[yB + zB] \leqq E_xE_yE_z x(B),$$

where now $0 \leqq B \leqq I$. Write $Q = E_xE_yE_z$. Since $\lambda(Q) > 1 - \epsilon$, we have

$$\lambda(B) \geqq \lambda(QxB) = \lambda(QyB) + \lambda(QzB) \geqq \lambda(yB) + \lambda(zB) - 2\epsilon$$
$$= 2\lambda(B) - 2\epsilon.$$

This gives the inequality

$$(8.8) \qquad \lambda(B) \leqq 2\epsilon.$$

On the other hand, using condition (1) of the proposition, $T \leqq \sum_{u \in F} E_u + \sum_{u \in F} E_{xu}$. Therefore, $E_xT \leqq E_xA + E_x xA$, and applying (8.6), we have

$$(8.9) \qquad E_x \leqq E_xB + E_x xB.$$

Therefore, $\lambda(E_x) \leqq 2\lambda(B)$. But $\lambda(E_x) \geqq \lambda(Q) > 1 - \epsilon$, so

$$(8.10) \qquad \lambda(B) \geqq (1 - \epsilon)/2.$$

Inequalities (8.8) and (8.10) are inconsistent when $\epsilon < 1/5$. The proposition is proved.

The conditions of this proposition are not hard to realize. For example,

let K be the free product of three groups each or order two. If x, y and z denote the generators, and F is the set of all words (in reduced form) which begin with x, then it is clear that the conditions (1)-(3) hold. Further, Lemma 2.1 shows that this group has a faithful representation as a freely acting MP automorphism group. Therefore,

COROLLARY 8.1. *There exist countable discrete groups which have no faithful representations as freely acting approximately finite MP automorphism groups. In particular, there exist non-approximately finite automorphism groups.*

By Theorem 3, the free product of $n \geqq 3$ groups of order two (or for that matter, the group of all measure preserving transformations of (M, λ)) will be non-approximately finite. The free group on $n \geqq 2$ generators also satisfies the conditions of Proposition 8.1. It is of interest that the free product of two groups of order two is approximately finite, together with all abelian groups; these facts will be established in the course of further development of the theory.

UNIVERSITY OF SOUTHERN CALIFORNIA,
LOS ANGELES, CALIFORNIA.

REFERENCES.

[1] J. Dixmier, "Sur certains espaces consideres par M. H. Stone," *Summa Brasiliensis Mathematicae*, vol. 2 (1951), Fasc. 11.

[2] ———, *Les algebres d'operateurs dans l'espace hilbertien*, Paris, 1957.

[3] P. R. Halmos, "Approximation theories for measure preserving transformations," *Transactions of the American Mathematical Society*, vol. 55 (1944), pp. 1-18.

[4] S. Kakutani, "Concrete representations of abstract (M)-spaces," *Annals of Mathematics*, vol. 42 (1941), pp. 994-1024.

[5] I. Kaplansky, "Quelques resultats sur les anneaux d'operateurs," *Comptes Rendus Hebdomaire des Séances de l'Académie des Sciences*, Paris, vol. 123 (1950), pp. 485-486.

[6] D. Maharam, "On homogeneous measure algebras," *Proceedings of the National Academy of Sciences*, vol. 28 (1942), pp. 108-111.

[7] Y. Misonou, "Generalized approximately finite W^*-algebras," *Tôhoku Mathematical Journal*, vol. 7 (1955), pp. 192-205.

[8] F. J. Murray and J. von Neuman, "On rings of operators. IV," *Annals of Mathematics*, vol. 44 (1943), pp. 716-808.

[9] I. M. Singer, "Automorphisms of finite factors," *American Journal of Mathematics*, vol. 77 (1955), pp. 117-133.

[10] M. H. Stone, "Boundedness properties in function-lattices," *Canadian Journal of Mathematics*, vol. 1 (1949), pp. 176-186.

SUR LES REPRÉSENTATIONS UNITAIRES DES GROUPES DE LIE NILPOTENTS. I.*

Par J. Dixmier.

Introduction. Soient G un groupe localement compact, H un sous-groupe abélien fermé distingué de G, $\hat{H}$ le dual de H. Tout élément s de G définit un automorphisme $x \to sxs^{-1}$ de H, donc un automorphisme de $\hat{H}$. L'ensemble des transformés d'un point de $\hat{H}$ par G est une partie de $\hat{H}$ appelée orbite. Disons que H est *régulièrement contenu* dans G s'il existe une suite de parties boréliennes $E_1, E_2, \cdots$ de $\hat{H}$, stables pour G, telles que toute orbite soit l'intersection des E_i qui la contiennent. Cette notion est due à Mackey [6]. Nous démontrerons le théorème suivant:

Théorème 1. *Soient G un groupe de Lie réel connexe nilpotent, H un sous-groupe abélien fermé distingué connexe de G. Alors, H est régulièrement contenu dans G.*

On sait que la conclusion du théorème est inexacte lorsqu'on remplace l'hypothèse "G nilpotent" par l'hypothèse "G résoluble." D'autre part, on verra que la conclusion du théorème est également en défaut si H n'est pas supposé connexe. Enfin, un exemple inédit de Mackey montre qu'on ne peut supprimer l'hypothèse "G connexe."

Mackey a montré [6] que la notion de sous-groupe régulièrement contenu joue un rôle important dans la recherche des représentations unitaires d'un groupe. Grâce à ses résultats, nous déduirons du Théorème 1 les théorèmes suivants:

Théorème 2. *Soient G un groupe de Lie réel connexe nilpotent, H un sous-groupe abélien fermé distingué connexe de G, $s \to U_s$ une représentation unitaire factorielle continue de G dans un espace hilbertien. Il existe un sous-groupe fermé connexe $G' \supset H$ de G, et une représentation unitaire continue U' de G' par des opérateurs scalaires, tels que U soit unitairement équivalente à la représentation de G induite par U'.*

(Si U est irréductible, U' s'effectue nécessairement dans un espace de dimension 1.)

* Received August 24, 1958.

THÉORÈME 3.[1] *Toute représentation unitaire continue d'un groupe de Lie réel connexe nilpotent est de type* I.

Avant d'aborder les démonstrations, précisons quelques notations:

1° Une application f d'un ensemble A dans un ensemble B est dite injective si elle transforme deux éléments distincts en éléments distincts, surjective si $f(A)=B$, bijective si elle est injective et surjective;

2° Soit R une relation d'équivalence sur un ensemble X, et soit X' une partie de X. On désigne par $R_{X'}$ la relation d'équivalence induite par R dans X';

3° Une relation d'équivalence R dans un espace topologique X est dite séparée si l'espace quotient X/R est séparé;

4° Quand nous parlons de variété algébrique, nous ne supposons pas l'irréductibilité. Soient V une variété algébrique, E un sous-ensemble de V. On note $\dim E$ la plus grande dimension des composantes irréductibles de l'adhérence de E dans V pour la topologie de Zariski (*cf.* [3] et [4] pour la topologie de Zariski).

1. Démonstration du Théorème 1.

LEMME 1.[2] *Soient V un variété algébrique complexe, G un groupe algébrique complexe irréductible opérant à gauche dans V, l'application $(x,s)\to sx$ de $V\times G$ dans V étant partout régulière. Considérons deux points de V comme équivalents s'ils sont transformés l'un de l'autre par un élément de G. Soit R la relation d'équivalence ainsi définie. Alors, il existe une suite finie $(V_i)_{0\leq i\leq n}$ de variétés algébriques contenues dans V possédant les propriétés suivantes:*

a) $\phi=V_0\subset V_1\subset\cdots\subset V_n=V$;

b) *chaque V_i est stable pour G;*

c) *la relation d'équivalence $R_{V_{i+1}-V_i}$ est séparée pour la topologie ordinaire* $(i=0,\cdots,n-1)$.

[1] Ce théorème résulte aussi de mon article "Sur les représentations unitaires des groupes de Lie algébriques," Ann. de l'Institut Fourier, 7 (1957), pp. 315-328 (d'ailleurs rédigé postérieurement au présent mémoire). Mais la démonstration donnée ici est beaucoup plus élémentaire. Le théorème résulte également de [9].

[2] Depuis que ce mémoire a été rédigé, des résultats beaucoup plus généraux que le Lemme 1 ont été obtenus par C. Chevalley (cf. son Traité de Géométrie Algébrique, à paraître).

Démonstration. Toutes les notions topologiques utilisées dans la démonstration de ce lemme se réfèrent à la topologie de Zariski, sauf mention expresse du contraire.

Nous procéderons par récurrence sur la dimension complexe m de V, en supposant le lemme établi pour les variétés de dimension $< m$.

Soient $C_1, \cdots, C_p$ les composantes irréductibles de V. Nous allons montrer (ce qui est d'ailleurs bien connu) que G laisse stable chaque C_i. Soit A l'intersection de C_i avec les C_j d'indice $j \neq i$; c'est une partie fermée de C_i rare dans C_i. Il suffit donc de montrer que, si x est un point de C_i non dans A, on a $Gx \subset C_i$. Or l'adhérence B de Gx dans V est irréductible. L'égalité $B = (B \cap C_1) \cup (B \cap C_2) \cup \cdots \cup (B \cap C_p)$ prouve que l'un des $B \cap C_j$ est égal à B, d'où $B \subset C_j$; alors, $x \in C_j$; comme $x \notin A$, on a $j = i$, d'où $B \subset C_i$, ce qui prouve notre assertion.

Il en résulte facilement qu'il suffit de prouver le lemme lorsque V est irréductible, ce que nous supposerons désormais.

L'application $\phi: (x, s) \to (x, sx)$ de $V \times G$ dans $V \times V$ est partout régulière, et $D_1 = \phi(V \times G)$ est le graphe de R. L'adhérence D de D_1 dans $V \times V$ est une variété algébrique irréductible; soit n sa dimension. L'ensemble D_1 contient une partie relativement ouverte de D ([3], exposé 7, th. 3). Donc $D - D_1$ est contenu dans une partie fermée F de D de dimension $n' < n$.

Pour tout $x \in V$, on désignera par V_x l'ensemble des éléments de $V \times V$ dont la première coordonnée est x. Pour tout $x \in V$, on a $\dim(V_x \cap D) \geqq n - m$ ([3], exposé 8, th. 3). D'autre part (loc. cit.), il existe un ensemble rare E' de V tel que, pour $x \notin E'$, on ait $\dim(V_x \cap F) \leqq n' - m$. Si $x \notin E'$, on a donc $\dim(V_x \cap F) < n - m$. Soit E l'ensemble des points $x \in V$ tels que $\dim V_x \cap (D - D_1) \geqq n - m$. Ce qui précède montre que E est rare dans V.

Montrons que E est stable par G. Soit $s \in G$. Soit S l'application bijective et birégulière de $V \times V$ dans $V \times V$ qui transforme (x, y) en (sx, y). Il est clair que $S(D_1) = D_1$, donc que $S(D) = D$. D'autre part $S(V_x) = V_{sx}$, et par suite $S(V_x \cap (D - D_1)) = V_{sx} \cap (D - D_1)$. Donc, si $x \in E$, on a $sx \in E$, ce qui prouve notre assertion.

Montrons que, si $(u, v) \in D$ et $(v, w) \in D_1$, on a $(u, w) \in D$. Soit $s \in G$ tel que $w = sv$. Soit S' l'application bijective et birégulière de $V \times V$ dans $V \times V$ qui transforme (x, y) en (x, sy). Il est clair que $S'(D_1) = D_1$, donc que $S'(D) = D$. Donc $(u, w) = S'((u, v)) \in D$.

Soient $x \in V - E$, $y \in V - E$ des éléments tels que $(x, y) \in D$. Nous allons montrer que $(x, y) \in D_1$. Raisonnant par l'absurde supposons $(x, y) \notin D_1$.

Si $w \in V$ est tel que $(y,w) \in D_1$, on a $(x,w) \in D$ d'après ce qui précède, et $(x,w) \notin D_1$ (car les relations $(x,w) \in D_1$ et $(y,w) \in D_1$ entraîneraient $(x,y) \in D_1$, contrairement à l'hypothèse), donc $(x,w) \in D - D_1$; donc la deuxième projection $\mathrm{pr}_2(V_x \cap (D - D_1))$ contient $\mathrm{pr}_2(V_y \cap D_1)$; donc $\dim V_x \cap (D - D_1) \geqq \dim V_y \cap D_1$; comme $x \notin E$, on en déduit que $\dim V_y \cap D_1 < n - m$; par ailleurs, comme $y \notin E$, on a $\dim V_y \cap (D - D_1) < n - m$; donc $\dim V_y \cap D < n - m$, ce qui est absurde. On a donc bien prouvé que $(x,y) \in D_1$.

Il en résulte que le graphe de la relation d'équivalence R_{V-E} est $[(V-E)\times(V-E)] \cap D$, donc est fermé dans $(V-E)\times(V-E)$ (au sens de Zariski, donc au sens ordinaire). Par ailleurs, R_{V-E} est une relation d'équivalence ouverte au sens de la topologie ordinaire puisqu'elle est définie par un groupe d'homéomorphismes de $V - E$. Donc ([2], chap. I, § 9, th. 2), R_{V-E} est séparée pour la topologie ordinaire. Soit A l'adhérence de E dans V (au sens de Zariski). Alors, A est stable pour G, R_{V-A} est séparée pour la topologie ordinaire, et $\dim A < \dim V$. Il suffit maintenant d'appliquer à A, dont la dimension est $< m$, l'hypothèse de récurrence.

Les Lemmes 2 et 3 nous permettront d'utiliser le Lemme 1 dans le domaine réel et non plus dans le domaine complexe.

LEMME 2. *Soient W un espace vectoriel réel de dimension finie, u un endomorphisme nilpotent de W, W' la complexification de W. Considérons iu comme un endomorphisme de W'. Si $x \in W$, $y \in W$ sont tels que* $(\exp(iu)) \cdot x = y$, *on a* $x = y$.

Démonstration. Le lemme est évident si la dimension n de W est égale à 1. Procédant par récurrence, supposons le lemme établi pour les dimensions $< n$. Il existe une base $(e_1, \cdots, e_n)$ de W et des nombres réels $\lambda_1, \cdots, \lambda_{n-1}$ tels que $ue_j = \lambda_j e_{j+1}$ pour $j = 1, \cdots, n-1$, et $ue_n = 0$. Soient $x = \xi_1 e_1 + \cdots + \xi_n e_n$, $y = \eta_1 e_1 + \cdots + \eta_n e_n$, les ξ_j et les η_j étant réels. Soit $W_j = \boldsymbol{R}e_j + \boldsymbol{R}e_{j+1} + \cdots + \boldsymbol{R}e_n$ ($\boldsymbol{R}$ étant le corps des nombres réels). On a $u^2(W_1) \subset W_3$, donc $y = (\exp(iu)) \cdot x \equiv x + iux \equiv \xi_1 e_1 + (\xi_2 + i\lambda_1\xi_1) e_2 \pmod{W_3}$. Donc $\lambda_1 \xi_1 = 0$. Si $\xi_1 = 0$, on a $x \in W_2$, $y \in W_2$, et W_2 est stable pour u, donc $x = y$ d'après l'hypothèse de récurrence. Si $\lambda_1 = 0$, $\boldsymbol{R}e_1$ et W_2 sont stables pour u, et la décomposition en somme directe $W = \boldsymbol{R}e_1 + W_2$ donne encore $x = y$ d'après l'hypothèse de récurrence.

LEMME 3. *Soient $\mathfrak{g}$ une algèbre de Lie réelle nilpotente de dimension finie, $\mathfrak{g}' = \mathfrak{g} + i\mathfrak{g}$ sa complexification, G' un groupe de Lie complexe connexe d'algèbre de Lie $\mathfrak{g}'$. Alors, tout élément de G' se met sous la forme* $(\exp iY)(\exp X)$, *où* $X \in \mathfrak{g}$, $Y \in \mathfrak{g}$.

Démonstration. Le lemme est évident si la dimension n de $\mathfrak{g}$ est égale à 1. Procédant par récurrence, supposons le lemme établi pour les dimensions $< n$. Il existe un idéal $\mathfrak{h}$ de dimension 1 de $\mathfrak{g}$; cet idéal est contenu dans le centre de $\mathfrak{g}$. Soient $\mathfrak{h}'$ la complexification de $\mathfrak{h}$, et H' le sous-groupe connexe de G' correspondant à $\mathfrak{h}'$. Alors, la complexification de $\mathfrak{g}/\mathfrak{h}$ s'identifie à $\mathfrak{g}'/\mathfrak{h}'$, et G'/H' est un groupe de Lie complexe connexe d'algèbre de Lie $\mathfrak{g}'/\mathfrak{h}'$. Soit $s \in G'$. D'après l'hypothèse de récurrence, il existe $X_1 \in \mathfrak{g}$, $Y_1 \in \mathfrak{g}$ tels que $(\exp iY_1)(\exp X_1)$ et s soient congrus modulo H'. Il existe donc $X_2 \in \mathfrak{h}$, $Y_2 \in \mathfrak{h}$ tels que $s = (\exp iY_1)(\exp X_1)(\exp iY_2)(\exp X_2)$. Comme X_2 et Y_2 sont dans le centre de $\mathfrak{g}$, ceci s'écrit $s = (\exp i(Y_1 + Y_2))(\exp(X_1 + X_2))$. D'où le lemme.

LEMME 4. *Soient $\mathfrak{g}$ une algèbre de Lie nilpotente réelle, V un espace vectoriel réel de dimension finie, ρ une représentation linéaire de $\mathfrak{g}$ dans V par des endomorphismes nilpotents, G un groupe de Lie réel connexe d'algèbre de Lie $\mathfrak{g}$, σ la représentation (qu'on suppose exister) de G dans V correspondant à ρ. Considérons deux points de V comme équivalents s'ils sont transformés l'un de l'autre par un automorphisme $\sigma(s)$, où $s \in G$. Soit R la relation d'équivalence ainsi définie. Alors, il existe une suite finie $(V_i)_{0 \leqq i \leqq n}$ de variétés algébriques réelles contenues dans V possédant les propriétés suivantes:*

a) $\phi = V_0 \subset V_1 \subset \cdots \subset V_n = V$;

b) *chaque V_i est stable pour G;*

c) *la relation d'équivalence $R_{V_{i+1}-V_i}$ est séparée* $(i = 0, \cdots, n-1)$.

Démonstration. Soient V', $\mathfrak{g}'$, ρ' les complexifications de V, $\mathfrak{g}$, ρ; soient G' le groupe de Lie complexe connexe simplement connexe d'algèbre de Lie $\mathfrak{g}'$, σ' la représentation de G' correspondant à ρ'. Considérons deux points de V' comme équivalents s'ils sont transformés l'un de l'autre par un automorphisme $\sigma'(s')$, où $s' \in G'$. Soit R' la relation d'équivalence ainsi définie. Il existe (Lemme 1) des variétés algébriques complexes $V'_0, \cdots, V'_n$ contenues dans V', avec $\phi = V'_0 \subset \cdots \subset V'_n$, stables pour G', telles que les relations d'équivalence $R'_{V'_{i+1}-V'_i}$ soient séparées. Alors, les $V_i = V'_i \cap V$ sont des variétés algébriques réelles stables pour G, telles que les relations d'équivalence $R'_{V_{i+1}-V_i}$ soient séparées. Il suffit donc de montrer que $R'_V = R$. Il est clair que deux points de V congrus modulo R sont aussi congrus modulo R'_V. Réciproquement, soient x, y deux points de V congrus modulo R'_V. Il existe $s' \in G'$ tel que $y = \sigma'(s')x$. D'après le Lemme 3, il existe $X \in \mathfrak{g}$,

$Y \in \mathfrak{g}$ tels que $s' = (\exp iY)(\exp X)$. Alors $y = \sigma'((\exp iY)(\exp X))x = (\exp i\rho(Y))(\exp \rho(X))x$. D'après le Lemme 2 appliqué à y et $(\exp \rho(X))x$, on a $y = (\exp \rho(X))x = \sigma(\exp X)x$. D'où le lemme.

Démonstration du Théorème 1. Soient G un groupe de Lie réel connexe nilpotent, H un sous-groupe abélien fermé distingué connexe, $\hat{H}$ le dual de G. Nous allons montrer que $H^{\cdot}$ est régulièrement contenu dans G. Soit K le plus grand sous-groupe compact de H. Il est invariant par tous les automorphismes de H, donc est distingué dans G. Soit L le groupe de recouvrement de H; c'est un espace vectoriel de dimension finie, et H est un quotient de L. Soit $\hat{L}$ le groupe dual de L; il s'identifie à l'espace vectoriel dual de l'espace vectoriel L, et $\hat{H}$ s'identifie à un sous-groupe fermé de $\hat{L}$.

Pour tout $s \in G$, soient $\tau(s)$ l'automorphisme $x \to sxs^{-1}$ de H, $\sigma'(s)$ l'automorphisme correspondant de L, $\sigma(s)$ l'automorphisme de $\hat{L}$ dual de $\sigma'(s)$. Alors, σ' est une représentation linéaire de G dans L qui laisse stable le noyau de l'application canonique de L sur H, donc σ est une représentation linéaire de G dans $\hat{L}$ qui laisse stable $\hat{H}$. Soient $\mathfrak{g}$ l'algèbre de Lie de G, $\mathfrak{h} \subset \mathfrak{g}$ l'algèbre de Lie de H, ou de L. Alors la représentation de $\mathfrak{g}$ correspondant à σ' est la représentation adjointe ρ' de $\mathfrak{g}$ dans $\mathfrak{h}$; elle s'effectue par des endomorphismes nilpotents. La représentation ρ de $\mathfrak{g}$ correspondant à σ est la transposée de ρ'; elle s'effectue également par des endomorphismes nilpotents. On est donc dans les conditions d'application du Lemme 4. Ce lemme entraîne que H est réunion de sous-ensembles boréliens deux à deux disjoints $B_1, \cdots, B_n$, stables pour G, possédant les propriétés suivantes: chaque B_i est un espace métrique à base dénombrable, et la relation d'équivalence définie par G dans chaque B_i est ouverte et séparée. Il en résulte aussitôt que H est régulièrement contenu dans G. D'où le Théorème 1.

Remarque. En fait, on déduit facilement de la démonstration que H est même "régulier dans G" au sens de F. Bruhat ("Sur les représentations induites des groupes de Lie," *Bull. Soc. Math. France*, vol. 84 (1956), pp. 97-205, définition 5.3).

2. Démonstration des Théorèmes 2 et 3.

LEMME 5. *Soient G un groupe de Lie réel connexe nilpotent, H un sous-groupe abélien fermé distingué connexe, $\hat{H}$ le dual de H, χ un élément de $\hat{H}$, S le stabilisateur de χ dans G. Alors, S est connexe.*

Démonstration. Nous conservons les notations de la démonstration précédente. Soit $s \in S$, et montrons que s appartient à un sous-groupe à un

paramètre de S. Puisque G est nilpotent, on a $s = \exp X$ avec un $X \in \mathfrak{g}$. Alors, $\sigma(s) = \exp \rho(X)$, et $\rho(X) = \sigma(s) - 1 - \frac{1}{2}(\sigma(s) - 1)^2 + \frac{1}{3}(\sigma(s) - 1)^3 - \cdots$ (les termes de la série étant nuls à partir d'un certain rang). Donc $\rho(X)\chi = 0$. Alors, $(\sigma(\exp(tX)))\chi = (\exp(t\rho(X)))\chi = \chi$ pour tout nombre réel t, d'où notre assertion.

LEMME 6. *Soit $\mathfrak{g}$ une algèbre de Lie nilpotente de dimension > 1. Tout idéal abélien maximal de $\mathfrak{g}$ est de dimension > 1.*

Démonstration. Soit $\mathfrak{h}$ un idéal de $\mathfrak{g}$ de dimension 1. D'après le théorème d'Engel, il existe une suite d'idéaux $(\mathfrak{h}_0, \mathfrak{h}_1, \cdots, \mathfrak{h}_n)$ de $\mathfrak{g}$ tels que $\mathfrak{h} = \mathfrak{h}_0 \subset \mathfrak{h}_1 \subset \cdots \subset \mathfrak{h}_n = \mathfrak{g}$, $\dim \mathfrak{h}_i/\mathfrak{h}_{i-1} = 1$, $[\mathfrak{g}, \mathfrak{h}_i] \subset \mathfrak{h}_{i-1}$. Soit $\mathfrak{k}$ un sous-espace de dimension 1 de $\mathfrak{h}_1$ tel que $\mathfrak{h}_1 = \mathfrak{h}_0 + \mathfrak{k}$. On a

$$[\mathfrak{h}_1, \mathfrak{h}_1] = [\mathfrak{h}_1, \mathfrak{h}_0] + [\mathfrak{k}, \mathfrak{k}] \subset [\mathfrak{g}, \mathfrak{h}_0] = 0,$$

donc $\mathfrak{h}_1$ est un idéal abélien contenant strictement $\mathfrak{h}_0$. D'où le lemme.

Démonstration du Théorème 2. Soient G un groupe de Lie réel connexe nilpotent, H un sous-groupe abélien fermé distingué connexe de G, $s \rightarrow U_s$ une représentation unitaire factorielle continue de G dans un espace hilbertien $\mathfrak{H}$.

a) Nous supposons d'abord que $\mathfrak{H}$ est à base dénombrable. Soient $\hat{H}$ le groupe dual de H, V la restriction de U à H, M le noyau de V, N la composante connexe de M. Il est clair que M est un sous-groupe fermé distingué de G, donc il en est de même de N.

Le théorème est évident si $H = G$. Soit $n = \dim G - \dim H$. Nous procéderons par récurrence sur n, en supposant le théorème démontré lorsque $\dim G - \dim H < n$.

D'après le Théorème 1, H est régulièrement contenu dans G. Puisque H est à base dénombrable, il existe ([6]) un point $\psi \in H$ possédant les propriétés suivantes: 1) si O est l'orbite de ψ relativement à G, la mesure sur H associée à la décomposition spectrale de V (théorème de Stone généralisé) est concentrée sur O; 2) si S est le stabilisateur de ψ dans G, U est unitairement équivalente à la représentation de G induite par une représentation unitaire factorielle continue W de S. Distinguons alors deux cas.

1) Si $O = \{\psi\}$, on a $H \subset S \neq G$, donc $\dim S - \dim H < \dim G - \dim H$. Comme S est connexe (Lemme 5) l'hypothèse de récurrence prouve qu'il existe un sous-groupe fermé connexe $G' \supset H$ de S et une représentation unitaire continue U' de G' par des opérateurs scalaires tels que W soit unitairement équivalente à la représentation de S induite par U'. Alors, d'après le théorème

sur les représentations induites par étages ([7], th. 4.1), U est unitairement équivalente à la représentation de G induite par U'.

2) Si $O=\{\psi\}$, on a $V(s)=\psi(s)\cdot 1$ pour $s\in H$, donc $\dim N$ est égal à $\dim H$ ou à $(\dim H-1)$. Supposons d'abord N réduit à l'élément neutre. Alors, H est de dimension 0 ou 1. Si $\dim G=1$, le théorème est évident. Si $\dim G>1$, le Lemme 6 prouve qu'il existe un sous-groupe abélien fermé distingué connexe H_1 de G contenant H tel que $\dim G-\dim H_1<\dim G-\dim H$. Le théorème résulte alors de l'hypothèse de récurrence. Venons-en au cas où N est quelconque. Soient $\tilde{G}=G/N$, $\tilde{H}=H/N$, $\tilde{U}$ la représentation factorielle de $\tilde{G}$ déduite de U par passage au quotient. D'après ce qu'on vient de voir, il existe un sous-groupe fermé connexe $\tilde{G}'$ contenant $\tilde{H}$ de $\tilde{G}$ et une représentation unitaire continue $\tilde{U}'$ de $\tilde{G}'$ par des opérateurs scalaires tels que $\tilde{U}$ soit unitairement équivalente à la représentation de $\tilde{G}$ induite par $\tilde{U}'$. Soient G' l'image réciproque de $\tilde{G}'$ dans G pour l'application canonique θ de G sur $\tilde{G}$, et $U'=\tilde{U}\cdot\theta$, qui est une représentation unitaire continue de G' par des opérateurs scalaires. Le groupe G' est fermé, contient H, et est connexe parce que N est connexe. Il est immédiat que U est unitairement équivalente à la représentation de G induite par U'. Ceci achève la démonstration lorsque $\mathfrak{H}$ est à base dénombrable.

b) Supposons maintenant que $\mathfrak{H}$ ne soit pas à base dénombrable. Soient x un élément non nul de $\mathfrak{H}$, et (s_j) une suite partout dense dans G. Les $U_{s_j}x$ engendrent un sous-espace vectoriel fermé non nul $\mathfrak{K}$ de $\mathfrak{H}$, stable pour U, et à base dénombrable. Soit A le facteur engendré par les opérateurs U_s, et soit A' le facteur commutant de A. D'après des résultats connus sur les algèbres de von Neumann (cf. par exemple [5], chap. III, § 1, cor. 2 du th. 1), il existe une famille $(\mathfrak{K}_i)_{i\in I}$ de sous-espaces vectoriels fermés de $\mathfrak{H}$, deux à deux orthogonaux, stables pour A, de somme hilbertienne $\mathfrak{H}$, et tous équivalents à $\mathfrak{K}$ relativement à A'. Soit W la représentation de G obtenue en restreignant à $\mathfrak{K}$ les opérateurs U_s. Alors, U est somme hilbertienne d'une famille $(W_i)_{i\in I}$ de représentations unitairement équivalentes à W. D'après la partie a) de la démonstration, il existe un sous-groupe fermé connexe $G'\supset H$ de G, et une représentation unitaire continue W' de G' par des opérateurs scalaires, tels que W soit unitairement équivalente à la représentation de G induite par W'. Pour tout $i\in I$, soit W'_i une représentation de G' unitairement équivalente à W', et U' la somme hilbertienne des W'_i. Alors ([7], th. 10.1), U est unitairement équivalente à la représentation de G induite par U'.

Démonstration du Théorème 3. Soient G un groupe de Lie réel connexe nilpotent, $s \to U_s$ une représentation unitaire continue de G dans un espace hilbertien $\mathfrak{H}$.

a) Supposons U factorielle et $\mathfrak{H}$ à base dénombrable. Soit n un entier > 0. Le théorème est évident pour les groupes abéliens. Supposons le théorème établi pour les groupes de Lie réels connexes nilpotents G possédant un sous-groupe abélien fermé distingué connexe H tel que $\dim G - \dim H < n$. Considérons alors le cas où G possède un sous-groupe abélien fermé distingué connexe H tel que $\dim G - \dim H = n$.

La marche de la démonstration est alors la même que pour le Théorème 2. Soient V la restriction de U à H, O l'orbite dans $\hat{H}$ associée à V, ψ un point de O, S le stabilisateur de ψ dans G. On sait que U est unitairement équivalente à la représentation de G induite par une représentation unitaire continue U' de S. En outre, les projecteurs du système d'imprimitivité associé à cette représentation induite proviennent de la décomposition spectrale de V, donc appartiennent à l'algèbre de von Neumann engendrée par les U_s, $s \in G$. D'après [6], no. 6, l'algèbre de von Neumann B formée des opérateurs permutables aux U'_s, $s \in S$, est donc isomorphe à l'algèbre de von Neuman A formée des opérateurs permutables aux U_s, $s \in G$.

1) Si $O \neq \{\psi\}$, on a $H \subset S \neq G$, donc $\dim S - \dim H < \dim G - \dim H$. Comme S est connexe (Lemme 5), l'hypothèse de récurrence prouve que U' est de type I. Donc B est de type I, donc A est de type I, donc U est de type I.

2) Si $O = \{\psi\}$, on a $V(s) = \psi(s) \cdot 1$ pour $s \in H$. Soit M le noyau de V, qui est un sous-groupe fermé distingué de G. Soient $\tilde{G} = G/M$, $\tilde{H} = H/M$. Alors, $\tilde{H}$ est de dimension 0 ou 1. Si $\tilde{G}$ est de dimension 1, les U_s $(s \in G)$ sont deux à deux permutables, et le théorème est évident. Si $\dim \tilde{G} > 1$, il existe (Lemme 6) un sous-groupe abélien fermé distingué connexe $\tilde{H}'$ de $\tilde{G}$, contenant $\tilde{H}$, et de dimension > 1. D'après l'hypothèse de récurrence, la représentation $\tilde{U}$ de G déduite de U par passage au quotient est de type I. Donc U elle-même est de type I.

b) Supposons toujours $\mathfrak{H}$ à base dénombrable, mais U quelconque. Soit $U_s = \int^{\oplus} U^{y}{}_s \, d\mu(y)$ la décomposition de U en représentations factorielles $s \to U^{y}{}_s$. D'après la partie a) de la démonstration, les représentations U^y sont de type I. Donc ([8], th. 2.6) U est de type I.

c) Envisageons enfin le cas général. Soit $(\mathfrak{H}_\iota)_{\iota \in I}$ une famille maximale

de sous-espaces vectoriels fermés non nuls de $\mathfrak{H}$, deux à deux orthogonaux, stables pour U, tels que les représentations U_i obtenues en restreignant U aux $\mathfrak{H}_i$ soient de type I. On va montrer que $\mathfrak{H} = \bigoplus_{i \in I} \mathfrak{H}_i$. Raisonnant par l'absurde, supposons qu'il existe un élément $x \neq 0$ de $\mathfrak{H}$ orthogonal aux $\mathfrak{H}_i$. Soit (s_j) une suite partout dense dans G. Les $U_{s_j} x$ engendrent un sous-espace vectoriel fermé non nul $\mathfrak{K}$ de $\mathfrak{H}$, stable pour U, orthogonal aux $\mathfrak{H}_i$, et à base dénombrable. D'après la partie b) de la démonstration, la représentation obtenue en restreignant U à $\mathfrak{K}$ est de type I. Ceci contredit la maximalité de la famille $(\mathfrak{H}_i)_{i \in I}$. Donc $\mathfrak{H} = \bigoplus_{i \in I} \mathfrak{H}_i$. Il est alors bien connu que U est de type I (cf. par exemple [5], chap. III, § 2, exerc. 5a)). Ceci achève la démonstration.

COROLLAIRE DU THÉORÈME 3. *Toute représentation unitaire projective continue d'un groupe de Lie réel connexe nilpotent G est de type I.*

Démonstration. Soit U une telle représentation. On peut supposer G simplement connexe. D'après [1], U provient par passage au quotient d'une représentation unitaire continue d'un groupe de Lie réel connexe G', extension centrale de G. Alors, G' est nilpotent, donc U est de type I.

3. Un contre-exemple. Nous allons construire un groupe de Lie réel connexe nilpotent G et un sous-groupe fermé abélien *non* connexe H de G, tels que H ne soit pas régulièrement contenu dans G.

Soient $\boldsymbol{R}$ le groupe additif des nombres réels, $\boldsymbol{Z}$ le sous-groupe des entiers rationnels, et $\boldsymbol{T} = \boldsymbol{R}/\boldsymbol{Z}$. Définissons sur $\boldsymbol{R}^4$ une multiplication de la manière suivante:

$$(x_1, x_2, x_3, x_4)(y_1, y_2, y_3, y_4)$$
$$= (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4 - x_2 y_1 - 2^{\frac{1}{2}} x_3 y_1).$$

On vérifie aisément que cette multiplication est associative, que $(0, 0, 0, 0)$ est élément neutre, et que $(-x_1, -x_2, -x_3, -x_4 - x_1 x_2 - 2^{\frac{1}{2}} x_1 x_3)$ est inverse de (x_1, x_2, x_3, x_4). On a donc défini un groupe de Lie réel G, connexe. Les éléments dont les trois premières coordonnées sont nulles forment un sous-groupe C. On a la formule

$$(1) \quad (x_1, x_2, x_3, x_4)(y_1, y_2, y_3, y_4)(x_1, x_2, x_3, x_4)^{-1}$$
$$= (y_1, y_2, y_3, y_4 + x_1 y_2 - x_2 y_1 + 2^{\frac{1}{2}}(x_1 y_3 - x_3 y_1)).$$

Sur la formule (1), on voit que C est central; comme G/C est évidemment abélien, G est nilpotent.

Soit H l'ensemble des $(x_1, x_2, x_3, x_4) \in G$ tels que x_1 soit nul et x_2, x_3 entiers. Alors, H est un sous-groupe fermé distingué de G, abélien puisque

$$(0, x_2, x_3, x_4)(0, y_2, y_3, y_4) = (0, x_2 + y_2, x_3 + y_3, x_4 + y_4).$$

Soient $x = (0, y_2, y_3, y_4) \in H$, $s = (x_1, x_2, x_3, x_4) \in G$, et $sxs^{-1} = (0, y_2', y_3', y_4') \in H$. La formule (1) prouve que

$$y_2' = y_2 \qquad y_3' = y_3 \qquad y_4' = y_4 + x_1 y_2 + 2^{\frac{1}{2}} x_1 y_3.$$

Le dual $\hat{H}$ de H s'identifie à $\boldsymbol{T} \times \boldsymbol{T} \times \boldsymbol{R}$. Si $(\theta_2, \theta_3, \xi_4) \in H$ (où $\theta_2 \in \boldsymbol{T}, \theta_3 \in \boldsymbol{T}$, $\xi_4 \in \boldsymbol{R}$), son transformé par s est $(\theta_2', \theta_3', \xi')$, avec $\theta_2' = \theta_2 + x_1\xi_4$, $\theta_3' = \theta_3 + 2^{\frac{1}{2}} x_1 \xi_4$, $\xi_4' = \xi_4$.

Dans chaque sous-ensemble A_ξ de $\hat{H}$ défini par une valeur ξ de ξ_4, le groupe G agit ergodiquement pour la mesure de Haar de $\boldsymbol{T}^2$ (à cause de l'irrationnalité de $2^{\frac{1}{2}}$). Les parties de $\hat{H}$ mesurables pour la mesure de Haar de $\hat{H}$ et stables pour G sont donc, à des ensembles négligeables près, des réunions d'ensembles A_ξ. Ainsi, H n'est pas régulièrement contenu dans G.

INSTITUT HENRI POINCARÉ.

BIBLIOGRAPHIE.

[1] V. Bargmann, "On unitary ray representations of continuous groups," *Annals of Mathematics*, vol. 59 (1954), pp. 1-46.

[2] N. Bourbaki, *Topologie générale*, chap. I-II, 2e éd., Actualités Scientifiques et Industrielles, Paris, Hermann, 1951.

[3] H. Cartan et C. Chevalley, *Séminaire de géométrie algébrique*, miméographié, Paris, 1956.

[4] C. Chevalley, *Théorie des groupes de Lie*, tome III, Actualités Scientifiques et Industrielles, Paris, Hermann, 1955.

[5] J. Dixmier, *Les algèbres d'opérateurs dans l'espace hilbertien*, Paris, Gauthier-Villars, 1957.

[6] G. W. Mackey, "Imprimitivity for representations of locally compact groups," *Proceedings of the National Academy of Sciences of the U.S.A.*, vol. 35 (1949), pp. 537-545.

[7] ———, "Induced representations of locally compact groups," *Annals of Mathematics*, vol. 55 (1952), pp. 101-139.

[8] ———, "Induced representations of locally compact groups II. The Frobenius reciprocity theorem," *ibid.*, vol. 58 (1953), pp. 193-221.

[9] O. Takenouchi, "Sur la facteur-représentation d'un groupe de Lie résoluble de type (*E*)," *Mathematical Journal of Okayama University*, vol. 7 (1957), pp. 151-161.

GEOMETRIC SYZYGIES.* †

By G. Washnitzer.

The explanation of the title is that we give here a systematic interpretation of an exact sequence of sheaves in terms of geometric entities. In particular, we examine from this standpoint Hilbert's theorem concerning "chains of syzygies," and this provides an axiomatic characterization of the arithmetic genus of a non-singular projective model.

Given a coherent, algebraic, locally free sheaf E defined on a variety X, we attach a projective fiber bundle $\mathcal{B}(E)$, the "dual projective bundle" of E, whose base space is X. The fiber of $\mathcal{B}(E)$ is a projective space of dimension $n-1$, where n is equal to the dimension of the fiber of the vector bundle whose sheaf of germs of (algebraic) cross-sections is the sheaf E; in fact, the fiber of $\mathcal{B}(E)$ is equal to projective space formed by the vector subspaces of dimension $n-1$ in the fiber of the vector bundle. Let π_E denote the bundle projection of $\mathcal{B}(E)$ and let $\pi_E E$ denote the reciprocal image sheaf of E with respect to π_E, so that $\pi_E E$ is a locally free sheaf of dimension n defined on $\mathcal{B}(E)$. We construct a locally free sheaf $B(E)$ of dimension one defined on $\mathcal{B}(E)$ and a homomorphism from $\pi_E E$ onto $B(E)$. The kernel of this homomorphism is a locally free sheaf δE of dimension $n-1$ defined on $\mathcal{B}(E)$ and we have the following exact sequence of locally free sheaves defined on $\mathcal{B}(E)$:

$$0 \to \delta E \to \pi_E E \to B(E) \to 0.$$

$B(E)$ (resp. δE) is called the "basic sheaf" (resp. "derived sheaf") of the sheaf E. Assuming that X is non-singular (this is always the assumption in the text), we have that $B(E)$ is necessarily isomorphic with the sheaf of germs of rational functions on $\mathcal{B}(E)$ which are multiples of some divisor ϑ on $\mathcal{B}(E)$. The divisor class $\Theta(E)$ of ϑ depends solely upon the sheaf E, and $\Theta(E)$ is called the "basic class" of E.

Let E, G be locally free sheaves defined on X, and let ψ be a homomorphism from G into E with the property that the image sheaf $\mathrm{Im}[\psi\colon G \to E]$ is not the zero sheaf. Then we construct a rational transformation $\mathcal{B}(\psi)$

* Received May 6, 1958.

† This work was partially supported by the National Science Foundation.

from $\mathcal{B}(E)$ to $\mathcal{B}(G)$; $\mathcal{B}(\psi)$ is called the "dual rational transformation" of the homomorphism ψ. Let $\mathcal{G}(\psi)$ denote the graph of $\mathcal{B}(\psi)$ and let $\psi_{;1}$, $\psi_{;2}$ denote the projections from $\mathcal{G}(\psi)$ onto $\mathcal{B}(E)$, $\mathcal{B}(G)$ respectively. We pass to sheaves $\psi_{;1}B(E)$, $\psi_{;2}B(G)$, the reciprocal images of $B(E)$ and $B(G)$ with respect to $\psi_{;1}$ and $\psi_{;2}$ respectively, which are both locally free sheaves of dimension one defined on $\mathcal{G}(\psi)$. We then construct a locally free sheaf $S(\psi)$ of dimension one defined on $\mathcal{G}(\psi)$ and an isomorphism of the tensor product sheaf $\psi_{;2}B(G)\otimes S(\psi)$ onto $\psi_{;1}B(E)$.

A grave difficulty now arises. For, it can occur, in the absence of any further hypotheses, that the variety $\mathcal{G}(\psi)$ has multiple points; we can assume that X is non-singular. Furthermore, it can, and does indeed, occur that $\mathcal{G}(\psi)$ is non-singular, but that its projection into $\mathcal{B}(G)$ has multiple points. These possibilities present a serious obstacle to any detailed examination of the rational transformation $\mathcal{B}(\psi)$. Fortunately, there are some special cases which can be analyzed completely and which are of sufficient scope to cover a wide range of application.

Consider the case of an exact sequence

$$0\rightarrow H\xrightarrow{\theta} G\xrightarrow{\psi} E\rightarrow 0$$

of locally free sheaves defined on X. In this case, $\mathcal{B}(\psi)$ is a bi-regular mapping from $\mathcal{B}(E)$ onto a subvariety on $\mathcal{B}(G)$. Identifying $\mathcal{B}(E)$ with that subvariety, we have that the restriction of π_G to $\mathcal{B}(E)$ is equal to π_E, and that the trace of the divisor class $\Theta(G)$ on $\mathcal{B}(E)$ is equal to $\Theta(E)$. The graph $\mathcal{G}(\theta)$ is a non-singular variety; it is obtained by performing monoidal transformation on $\mathcal{B}(G)$ with the subvariety $\mathcal{B}(E)$ for center and the projection $\theta_{;1}$ is the anti-monoidal transformation. The projection $\theta_{;2}$ from $\mathcal{G}(\theta)$ to $\mathcal{B}(H)$ equips $\mathcal{G}(\theta)$ with the structure of the dual projective bundle of a certain locally free sheaf defined on $\mathcal{B}(H)$. In the present situation, we have that

$$\Theta(\theta_{;2}B(H))+\Theta(S(\theta))=\Theta(\theta_{;1}B(G)),$$

where the basic class $\Theta(S(\theta))$ of $S(\theta)$ is the divisor class of the anti-center $\mathcal{N}_\theta$ of $\theta_{;1}$; $\mathcal{N}_\theta$ is, of course, a non-singular subvariety of co-dimension one on $\mathcal{G}(\theta)$.

Next, let ψ be a homomorphism from G into E with the following property: The residue class sheaf Q of E modulo $\mathrm{Im}[\psi\colon G\rightarrow E]$ has for support a non-singular proper subvariety V on X, and Q is the extension to

X of a locally free sheaf defined on the subvariety V; thus we have the exact sequence

$$G \xrightarrow{\psi} E \xrightarrow{\phi} Q \to 0,$$

where ϕ is the quotient mapping from E to Q. Now $\mathcal{B}(Q)$ is a projective fiber bundle whose base space is V. In the first instance, $\mathcal{B}(\phi)$ makes no sense since Q is not a locally free sheaf on X; but we can define, in a natural way, a bi-regular mapping $\mathcal{B}(\phi)$ of $\mathcal{B}(Q)$ onto a non-singular subvariety on $\mathcal{B}(E)$. Identifying $\mathcal{B}(Q)$ with that subvariety, we have that the restriction of π_E to $\mathcal{B}(Q)$ is equal to π_Q and that the trace of $\Theta(E)$ on $\mathcal{B}(Q)$ is equal to $\Theta(Q)$. The graph $\mathcal{G}(\psi)$ is obtained by performing monoidal transformation on $\mathcal{B}(E)$ with the subvariety $\mathcal{B}(Q)$ for center; hence, $\mathcal{G}(\psi)$ is a non-singular variety and $\psi_{;1}$ is the anti-monoidal transformation. On the other hand, the subvariety on $\mathcal{B}(G)$ obtained by applying the projection $\psi_{;2}$ to $\mathcal{G}(\psi)$ has multiple points except for the following cases.

(a) V is a subvariety of co-dimension one on X.

(b) The dimension of the locally free sheaf Q on V is equal to the dimension of the locally free sheaf E on V.

Consider the case (a). Since V is of co-dimension one the kernel of ψ is a locally free sheaf defined on X, so that there is no loss of generality if we confine our attention to an exact sequence

$$0 \to G \xrightarrow{\psi} E \xrightarrow{\phi} Q \to 0$$

—E, G, locally free sheaves on X, Q is the extension of a locally free sheaf defined on V, V is a non-singular subvariety of co-dimension one on X. In this case, we prove that $\psi_{;2}$ is an anti-monoidal transformation from $\mathcal{G}(\psi)$ onto $\mathcal{B}(G)$; the center is a non-singular subvariety on $\mathcal{B}(G)$. Again we have that

$$\Theta(\psi_{;2}B(G)) + \Theta(S(\psi)) = \Theta(\psi_{;1}B(E)),$$

where $\Theta(S(\psi))$ is the divisor class of $\mathfrak{N}_\psi$; $\mathfrak{N}_\psi$ is a non-singular subvariety of co-dimension one on $\mathcal{G}(\psi)$ and it is the anti-center of $\psi_{;1}$. There is a detailed description of $\psi_{;2}$ in the text (§ 19).

Consider the following exact sequence of sheaves defined on a non-singular variety X:

$$F_t \to \cdots \to F_s \xrightarrow{\psi_s} F_{s-1} \to \cdots \to F_0 \xrightarrow{\psi_0} Q \to 0,$$

where $F_0, \cdots, F_t$ are locally free sheaves defined on X and Q is the extension to X of a locally free sheaf defined on V; V is a non-singular proper subvariety on X. Set $r = \dim. X$, $d = \dim. V$. Then, from the local version of Hilbert's syzygies theorem, it is well known that $\operatorname{Ker}[\psi_s : F_s \to F_{s-1}]$ is a locally free sheaf on X if $s \geqq r-d-1$. Consequently, there exist exact sequences

$$0 \to F_{r-d} \xrightarrow{\psi_{r-d}} \cdots \to F_s \xrightarrow{\psi_s} F_{s-1} \to \cdots \xrightarrow{\psi_0} Q \to 0,$$

where $F_0, \cdots, F_{r-d}$ are locally free; such exact sequences are called "resolutions" of Q by locally free sheaves. The foregoing discusssion permits the introduction of a "geometric resolution." One replaces each sheaf by its dual projective bundle, and each homomorphism by its dual rational transformation. However, we must use the following device so as to avoid the intractable cases where the "graphs" $\mathcal{G}(\psi_s)$ admit multiple points. Let X^* be obtained by performing monoidal transformation to X centered on V, let Φ denote the anti-monoidal transformation from X^* onto X, and V^* denote the anti-center, so that V^* is a non-singular subvariety of dimension $r-1$ on X^*. We set

$$F_s^* = \Phi F_s,$$
$$Q^* = \Phi Q,$$

so that F_s^* (resp. Q^*) is a locally free sheaf defined on X^* (resp. V^*), and we let

$$\psi_s^* : F_s^* \to F_{s-1}^*, \qquad 1 \leqq s \leqq r-d,$$
$$\psi_0^* : F_0^* \to Q^*,$$

where ψ_s^* is the reciprocal image of ψ_s with respect to Φ (see §§ 1, 2). The diagram of sheaves and homomorphisms on X^*

$$0 \to F_{r-d}^* \xrightarrow{\psi_{r-d}^*} \cdots \to F_s^* \xrightarrow{\psi_s^*} F_{s-1}^* \to \cdots \to F_0^* \to Q^* \to 0$$

is not exact if $d > 1$; but for $d > 1$, the following is true:

$$\operatorname{Ker}[\psi_s^*], \qquad 0 \leqq s \leqq r-d-1,$$
$$\operatorname{Im}[\psi_s^*], \qquad 1 \leqq s \leqq r-d,$$

are locally free sheaves on X^*; we have the exact sequences

$$0 \to \operatorname{Ker}[\psi_s^*] \to F_s^* \to \operatorname{Im}[\psi_s^*] \to 0, \qquad 1 \leqq s \leqq r-d-1,$$

of locally free sheaves defined on X^*; and the exact sequences

$$0 \to \operatorname{Im}[\psi_1^*] \to F_0^* \to Q^*$$
$$0 \to \operatorname{Im}[\psi_{s+1}^*] \to \operatorname{Ker}[\psi_s^*] \to Q^* \otimes \wedge^s(\delta N) \to 0, \qquad 1 \leqq s \leqq r - d - 1.$$

The sheaf δN is the derived sheaf of the locally free sheaf $N(X; V)$ of dimension $r - d$ on V of germs of cross-sections of covariant normal vector fields to V (see § 9); $\wedge^s(\delta N)$ is the s-fold exterion product of δN, and we recall that δN is a locally free sheaf of dimension $r - d - 1$ defined on V^*.

Chapter IV is an application of the method of "geometric resolution." We operate with an axiomatically defined "arithmetic functional" $\mathfrak{a}$ which assigns a rational number $\mathfrak{a}(X)$ to each non-singular projective model X. The decisive axiom (§ 21) is the Fiber Law:

(a) If Y is the dual projective bundle of a locally free sheaf defined on a non-singular projective model X. Then $\mathfrak{a}(X) = \mathfrak{a}(Y)$.

(b) If Y is obtained by performing monoidal transformation of a non-singular projective model X with center on a non-singular subvariety V, then $\mathfrak{a}(Y) = \mathfrak{a}(X)$. We proceed to prove that $\mathfrak{a}$ is unique by showing that $\mathfrak{a}(X) = \chi(X, \mathcal{O}_X)$, the Euler-Poincaré characteristic of the sheaf $\mathcal{O}_X$ of local rings on X. The equality $\mathfrak{a}(X) = \chi(X, \mathcal{O}_X)$ is proved merely on the assumption that $\mathfrak{a}$ exists, and we are not required to know that χ satisfies the Fiber Law. Indeed, χ does satisfy the Fiber Law; this being well known for non-singular varieties defined over a field of characteristic zero, and it has been proved by J. H. Sampson and the author for arbitrary characteristic.

We prefer, however, to establish the existence of an arithmetic functional along other lines. In a subsequent publication, we shall demonstrate that the Todd genus $T(X)$ satisfies the axioms; hence, we obtain

$$T(X) = \chi(X, \mathcal{O}_X)$$

which is the Todd-Hirzebruch formula for (non-singular) varieties defined over fields of arbitrary characteristic.

The contents of this paper were presented to a seminar at The Johns Hopkins University, April-May, 1957.

The principal references for the investigations of the present paper are the following articles:

[1] H. Cartan, "Extension du theoreme des "chaines de syzygies," *Rendiconti di Matematico* (Rome), vol. 11 (1952), pp. 156-166.

[2] D. Hilbert, "Über die Theorie der algebraischen Formen," *Mathematische Annalen*, vol. 36 (1890), pp. 473-534.

[3] J.-P. Serre, "Faiseaux algebriques coherents," *Annals of Mathematics*, vol. 61 (1955), pp. 197-278.

[4] A. Weil, *Fibre spaces in algebraic geometry*, University of Chicago (mimeographed notes).

[5] O. Zariski, "Foundations of a general theory of birational correspondences," *Transactions of the American Mathematical Society*, vol. 53 (1943), pp. 490-542.

[6] ———, "Complete linear systems on normal varieties and a generalization of a lemma of Enriques-Severi," *Annals of Mathematics*, vol. 55 (1952), pp. 552-592.

I. The Dual Projective Bundle and the Basic Sheaf of a Locally Free Sheaf.

§ 0. The term "variety" will refer always to an irreducible algebraic variety defined over a fixed algebraically closed field K of arbitrary characteristic. Our varieties are all equipped with the Zariski topology (with reference to K of course), and whenever we say that a variety is a subvariety on some other variety, we shall understand that the former is a closed subset on the latter. Every variety under consideration here will be either (a) a projective model (i. e., a subvariety on some projective space), or (b) it will admit a bi-regular correspondence onto an open subset of some projective model. There is, however, one instance where we construct a variety which a priori is merely an abstract variety; but we prove that this variety admits a bi-regular correspondence onto some projective model.

The term "sheaf" will always refer to a coherent algebraic sheaf defined on some variety, and a homomorphism of such sheaves will always be an algebraic homomorphism.

§ 1. U, V are varieties; Φ is a rational transformation from V to U. The graph of Φ is a subvariety Z on the product variety $V \times U$. We assume that Φ is regular. This means that for every point $\mathfrak{q}$ on V, there is one and only one point $\mathfrak{z} = (\mathfrak{q}, \mathfrak{p})$ on Z which projects onto $\mathfrak{q}$, and that the induced homomorphism of the local ring $\mathcal{O}_{\mathfrak{q}}$ of V at $\mathfrak{q}$ into the local ring $\mathcal{O}_{\mathfrak{z}}$ of Z at $\mathfrak{z}$ is an isomorphism of the former ring onto the latter. Let $\mathfrak{p}$ be the

point of U which is the image of $\mathfrak{s}$ by the projection from Z to U. Then we have that Φ induces a homomorphism $\Phi_{\mathfrak{q}}$ of the local ring $\mathcal{O}_{\mathfrak{p}}$ of U at $\mathfrak{p}$ into $\mathcal{O}_{\mathfrak{q}}$, and we set $\mathfrak{p} = \Phi(\mathfrak{q})$. Φ, as mapping of topological spaces, is a continuous map from V to U. We recall that the set theoretic image of V in U by Φ is not necessarily a closed subset on U.

We equip $\mathcal{O}_{\mathfrak{q}}$ with the structure of an $\mathcal{O}_{\mathfrak{p}}$-module according to the rule

$$u \cdot v = \Phi_{\mathfrak{q}}(u)v, \qquad u \in \mathcal{O}_{\mathfrak{p}},\ v \in \mathcal{O}_{\mathfrak{q}},$$

where the right hand side is a product in the ring $\mathcal{O}_{\mathfrak{q}}$. Now let A be a (coherent, algebraic) sheaf defined on U, and let $A_{\mathfrak{p}}$ be the stalk of A at $\mathfrak{p} = \Phi(\mathfrak{q})$. We form the $\mathcal{O}_{\mathfrak{p}}$-tensor product

$$\mathcal{O}_{\mathfrak{q}} \otimes_{\mathcal{O}_{\mathfrak{p}}} A_{\mathfrak{p}};$$

this being permissible since we have equipped $\mathcal{O}_{\mathfrak{q}}$ with the structure of an $\mathcal{O}_{\mathfrak{p}}$-module in a specific way. For notational convenience, let us set

$$A^*_{\mathfrak{q}} = \mathcal{O}_{\mathfrak{q}} \otimes_{\mathcal{O}_{\mathfrak{p}}} A_{\mathfrak{p}}.$$

We have a canonical $\mathcal{O}_{\mathfrak{p}}$-homorphism $\Phi^*_{\mathfrak{q}}$ of $A_{\mathfrak{p}}$ into the $\mathcal{O}_{\mathfrak{p}}$-module $A^*_{\mathfrak{q}}$ defined according to

$$\Phi^*_{\mathfrak{q}}(ua) = 1 \otimes (ua) = \Phi_{\mathfrak{q}}(u) \otimes a, \qquad u \in \mathcal{O}_{\mathfrak{p}}, a \in A_{\mathfrak{p}}.$$

On the other hand, $A^*_{\mathfrak{q}}$ carries the structure of an $\mathcal{O}_{\mathfrak{q}}$-module according to the rule

$$v_1(v_2 \otimes a) = (v_1 v_2) \otimes a, \qquad v_1, v_2 \in \mathcal{O}_{\mathfrak{q}}, a \in A_{\mathfrak{p}}.$$

The $\mathcal{O}_{\mathfrak{p}}$-homomorphism $\Phi^*_{\mathfrak{q}}$ maps any set of generators of $A_{\mathfrak{p}}$ onto a set of generators for $A^*_{\mathfrak{q}}$ viewed as $\mathcal{O}_{\mathfrak{q}}$-module. If $A_{\mathfrak{p}}$ is a free $\mathcal{O}_{\mathfrak{p}}$-module of dimension n, then $A^*_{\mathfrak{q}}$ is a free $\mathcal{O}_{\mathfrak{q}}$-module of dimension n.

§ 2. Set

$$A^* = \bigcup_{\mathfrak{q} \in V} A^*,$$

the disjoint union of the various modules $A^*_{\mathfrak{q}}$ for all $\mathfrak{q} \in V$. We shall prove that the set A^* carries the structure of one and only one coherent algebraic sheaf ΦA defined on V with the following properties:

(a) The stalk of ΦA at any point $\mathfrak{q}$ is the module $A^*_{\mathfrak{q}}$;

(b) Let γ be a section of A over an open set W on U, then the mapping $\Phi^{-1}\gamma$ which assigns to each point $\mathfrak{q}$ on $\Phi^{-1}(W)$ ($\Phi^{-1}(W)$ is the open set on V consisting of all points $\mathfrak{q}$ such that $\Phi(\mathfrak{q})$ is in W, and we assume that $\Phi^{-1}(W)$

is non-empty) the element $\Phi^*_{\mathfrak{q}}(\gamma(\mathfrak{p}))$ in $A^*_{\mathfrak{q}}$ ($\gamma(\mathfrak{p})$) is the value of γ in $A_{\mathfrak{p}}$, where $\mathfrak{p}=\Phi(\mathfrak{q})$, and $\Phi^*_{\mathfrak{q}}$ is the previous canonical homomorphism of $A_{\mathfrak{p}}$ into $A^*_{\mathfrak{q}}$) is a section of ΦA over $\Phi^{-1}(W)$. The sheaf ΦA is called the reciprocal image of A with respect to the mapping Φ.

It is clear that any two sheaves defined on V which satisfy both (a) and (b) must be identical. It remains for us to construct the sheaf ΦA. First, we observe that the reciprocal image of the sheaf $\mathcal{O}_U$ of local rings on U is the sheaf $\mathcal{O}_V$ of local rings on V. More generally, if A is a free sheaf of dimension n on U (i.e., A is isomorphic with the direct sum of $\mathcal{O}_U$ taken n times), then ΦA exists and it is a free sheaf of dimension n defined on V. Next, if A is such that we can choose free sheaves B, C defined on U and homomorphisms $\theta\colon C\to B$, $\psi\colon B\to A$ with the property that

$$C \xrightarrow{\theta} B \xrightarrow{\psi} A \to 0$$

is an exact sequence of sheaves defined on U, then ΦA exists. For in the present situation, we have the exact sequence

$$C_{\mathfrak{p}} \xrightarrow{\theta_{\mathfrak{p}}} B_{\mathfrak{p}} \xrightarrow{\psi_{\mathfrak{p}}} A_{\mathfrak{p}} \to 0$$

of stalks at any point $\mathfrak{p}=\Phi(\mathfrak{q})$ on U. Tensorize this exact sequence with $\mathcal{O}_{\mathfrak{q}}$ viewed as $\mathcal{O}_{\mathfrak{p}}$-module, thereby obtaining the exact sequence

$$C^*_{\mathfrak{q}} \xrightarrow{\theta^*_{\mathfrak{q}}} B^*_{\mathfrak{q}} \xrightarrow{\psi^*_{\mathfrak{q}}} A^*_{\mathfrak{q}} \to 0$$

of $\mathcal{O}_{\mathfrak{p}}$-modules; $B^*_{\mathfrak{q}}=\mathcal{O}_{\mathfrak{q}}\otimes_{\mathcal{O}_{\mathfrak{p}}}B_{\mathfrak{p}}$, $C^*_{\mathfrak{q}}=\mathcal{O}_{\mathfrak{q}}\otimes_{\mathcal{O}_{\mathfrak{p}}}C_{\mathfrak{p}}$ and $\theta^*_{\mathfrak{q}}=I_{\mathfrak{q}}\otimes\theta_{\mathfrak{p}}$, $\psi^*_{\mathfrak{q}}=I_{\mathfrak{q}}\otimes\psi_{\mathfrak{p}}$, where $I_{\mathfrak{q}}$ is the identity map of $\mathcal{O}_{\mathfrak{q}}$. We invoke here the well known fact that $\otimes_{\mathcal{O}_{\mathfrak{p}}}$ is a right exact functor. But this last exact sequence is clearly an exact sequence of $\mathcal{O}_{\mathfrak{q}}$-modules since $\theta^*_{\mathfrak{q}}$ and $\psi^*_{\mathfrak{q}}$ are $\mathcal{O}_{\mathfrak{q}}$-homomorphisms. The family of homomorphisms $\{\theta^*_{\mathfrak{q}}\}_{\mathfrak{q}\in V}$ defines an algebraic homomorphism $\Phi^{-1}(\theta)$ of ΦC into ΦB. Consider the quotient sheaf of ΦB modulo the image of ΦC by $\Phi^{-1}(\theta)$. The underlying set of this quotient sheaf can be indentified with A^* in a specific way, and performing this identification, we obtain the sheaf ΦA.

Finally, let A be an arbitrary coherent algebraic sheaf defined on U. Let W be an open set on U such that

1) $\Phi^{-1}(W)$ is non-empty,

2) There exist free sheaves B, C defined on W and homomorphisms $\theta\colon C \to B$, $\psi\colon B \to A$ such that

$$C \xrightarrow{\theta} B \xrightarrow{\psi} A \to 0$$

is an exact sequence. Let $A^*(W)$ be the subset of A^* consisting of the union of all $A^*_\mathfrak{q}$ with $\mathfrak{q} \in \Phi^{-1}(W)$. Then, by the previous discussion, $A^*(W)$ carries the structure of a coherent algebraic sheaf defined on $\Phi^{-1}(W)$, and this sheaf is the reciprocal image of the restriction of A to W with respect to the restriction of Φ to $\Phi^{-1}(W)$. If W' is another open set on U satisfying 1) and 2), then the restriction of the sheaf $A^*(W)$ to $\Phi^{-1}(W \cap W')$ is identical with the restriction of $A^*(W')$ to $\Phi^{-1}(W \cap W')$; for each of these last sheaves is the reciprocal image of the restriction of A to $W \cap W'$ by the restriction of Φ to $\Phi^{-1}(W \cap W')$. Since we can cover U by a family $\{W\}$ of open sets which satisfy 1) and 2), we obtain the sheaf ΦA defined on V.

Given an open set W on U, with $\Phi^{-1}(W)$ non-empty, there is a canonical homomorphism of the module $\Gamma(A, W)$ of sections of A over W into the module $\Gamma(\Phi A, \Phi^{-1}(W))$ of sections of ΦA over $\Phi^{-1}(W)$; this follows from condition (b) in the definition of ΦA. The module $\Gamma(\mathcal{O}_U, W)$ (resp. $\Gamma(\mathcal{O}_V, \Phi^{-1}(W))$) is the same as the ring of regular functions on W (resp. $\Phi^{-1}(W)$), and the canonical homomorphism of $\Gamma(\mathcal{O}_U, W)$ into $\Gamma(\mathcal{O}_V, \Phi^{-1}(W))$ is a ring homomorphism of the former ring into the latter. This permits us to view $\Gamma(\mathcal{O}_V, \Phi^{-1}(W))$ as module over $\Gamma(\mathcal{O}_U, W)$. More generally, $\Gamma(\Phi A, \Phi^{-1}(W))$ carries the structure of a $\Gamma(\mathcal{O}_U, W)$-module, and the canonical homomorphism of $\Gamma(A, W)$ into $\Gamma(\Phi A, \Phi^{-1}(W))$ is a $\Gamma(\mathcal{O}_U, W)$-homomorphism.

A, B are sheaves defined on U, and ψ is a homomorphism of B into A. We construct an $\mathcal{O}_\mathfrak{q}$-homomorphism $\psi^*_\mathfrak{q}$ of $B^*_\mathfrak{q}$ (the stalk of ΦB at $\mathfrak{q}$) into $A^*_\mathfrak{q}$ (the stalk of ΦA at $\mathfrak{q}$) according to the rule

$$\psi^*_\mathfrak{q}\colon v \otimes b \to v \otimes \psi_\mathfrak{p}(b), \qquad v \in \mathcal{O}_\mathfrak{q}, b \in B_\mathfrak{p},$$

where $\psi_\mathfrak{p}$ is the homomorphism of $B_\mathfrak{p}$ into $A_\mathfrak{p}$ assigned by ψ. One readily proves that the family of homomorphisms $\{\psi^*_\mathfrak{q}\}_{\mathfrak{q} \in V}$ gives a homomorphism $\Phi^{-1}(\psi)$ of ΦB into ΦA, which we call the reciprocal image of the homomorphism ψ. For any open set W on U, with $\Phi^{-1}(W)$ non-empty, we have the following commutative diagram.

$$\begin{array}{ccc}
\Gamma(B, W) & \longrightarrow & \Gamma(A, W) \\
\downarrow & & \downarrow \\
\Gamma(\Phi B, \Phi^{-1}(W)) & \to & \Gamma(\Phi A, \Phi^{-1}(W));
\end{array}$$

the horizontal arrows are induced by the sheaf homomorphisms ψ and $\Phi^{-1}(\psi)$; the vertical arrows are the aforementioned canonical homomorphisms.

The chief peculiarity with the notion of the reciprocal image of an algebraic sheaf is that exact sequences are not generally preserved. Given an exact sequence

$$0 \to C \xrightarrow{\theta} B \xrightarrow{\psi} A \to 0$$

of sheaves defined on U, then we have the exact sequence

$$\Phi C \xrightarrow{\Phi^{-1}(\theta)} \Phi B \xrightarrow{\Phi^{-1}(\psi)} \Phi A \to 0$$

of sheaves defined on V; but it is not always true that the kernel of $\Phi^{-1}(\theta)$ is the sheaf zero. Further on, we shall encounter some interesting examples where exactness fails to be preserved.

In the situation where V is a subvariety on U and Φ is the identity map of V in U, we shall call ΦA the induced sheaf of A on the subvariety V.

§ 3. X is a non-singular projective model, and E is a locally free sheaf of dimension n $(n > 0)$ defined on X (i.e., the stalk $E_{\mathfrak{p}}$ of E at any point $\mathfrak{p}$ on X is a free $\mathcal{O}_{\mathfrak{p}}$-module of dimension n). It is possible to choose an arbitrarily fine covering $\mathfrak{U} = \{U_\alpha\}_{\alpha \in J}$ of X consisting of finitely many non-empty open sets U_α on X such that:

1) Each U_α admits a bi-regular correspondence onto some affine model (i.e., a subvariety on some affine space),

2) The restriction of E to any U_α is a free sheaf of dimension n. Consequently, we can choose for each $\alpha \in J$ sections $e^\alpha{}_1, \cdots, e^\alpha{}_n$ of E over U_α such that for each $\mathfrak{p} \in U_\alpha$, the elements $e^\alpha{}_1(\mathfrak{p}), \cdots, e^\alpha{}_n(\mathfrak{p})$ generate $E_{\mathfrak{p}}$ as free $\mathcal{O}_{\mathfrak{p}}$-module of dimension n. For an ordered pair (α, β), we have that

$$e^\alpha{}_j = \sum_{i=1}^{n} E^\beta{}_i{}^\alpha{}_j e^\beta{}_i, \qquad 1 \leqq j \leqq n,$$

where the $E^\beta{}_i{}^\alpha{}_j$ are rational functions on X which are regular at each point of the set theoretic intersection $U_\alpha \cap U_\beta$. Thus for each point $\mathfrak{p}$ on $U_\alpha \cap U_\beta$, we have

$$e^\alpha{}_j(\mathfrak{p}) = \sum_{i=1}^{n} E^\beta{}_i{}^\alpha{}_j e^\beta{}_i(\mathfrak{p}),$$

where $E^\beta{}_i{}^\alpha{}_j$ is viewed as element of $\mathcal{O}_{\mathfrak{p}}$.

Let $E^{\beta\alpha}$ be the square matrix of order n whose entry in i-th row and j-th column is $E^\beta{}_i{}^\alpha{}_j$. Then we have the matrix product

$$E^{\alpha\gamma} E^{\gamma\beta} E^{\beta\alpha}$$

is equal to the unit matrix for any (α, β, γ), and that

$$E^{\alpha\beta}E^{\beta\alpha}$$

is also equal to the unit matrix. In particular, $\det E^{\beta\alpha}$ is a unit in the local ring of X at any point in $U_\alpha \cap U_\beta$. Reciprocally, if we are given a family of matrices with the above properties, then they serve as a system of transitions laws for a locally free sheaf defined on X which is unique up to isomorphism.

For each $\alpha \in J$, we choose a projective space P_α of dimension $n-1$ and fix a homogeneous coordinate system $\tau^\alpha_1, \cdots, \tau^\alpha_n$ for P_α. Form the product variety $U_\alpha \times P_\alpha$ and let π_α denote the coordinate projection from $U_\alpha \times P_\alpha$ onto U_α. Let $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$ be the open set on $U_\alpha \times P_\alpha$ consisting of all points which π_α maps on $U_\alpha \cap U_\beta$. We are going to construct a bi-regular mapping $\phi_{\beta\alpha}$ of $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$ onto $\pi_\beta^{-1}(U_\alpha \cap U_\beta)$. Let $\mathfrak{e}$ be a point $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$, then $\phi_{\beta\alpha}(\mathfrak{e})$ is that point of $\pi_\beta^{-1}(U_\alpha \cap U_\beta)$ such that

1) $\pi_\beta(\phi_{\beta\alpha}(\mathfrak{e})) = \pi_\alpha(\mathfrak{e}) = \mathfrak{p} \in U_\alpha \cap U_\beta$,

2) $\rho_1 \tau^\alpha_j(\mathfrak{e}) = \rho_2 \sum_{i=1}^{n} E^\beta{}_i{}^\alpha{}_j(\mathfrak{p}) \tau^\beta_i(\phi_{\beta\alpha}(\mathfrak{e}))$, $\qquad 1 \leqq j \leqq n.$

(ρ_1, ρ_2 are constants not both zero, and $E^\beta{}_i{}^\alpha{}_j(\mathfrak{p})$ is the value of the function $E^\beta{}_i{}^\alpha{}_j$ at $\mathfrak{p}$.) Since $\det E^{\beta\alpha}$ is a unit in the local ring $\mathcal{O}_\mathfrak{p}$ of X at any point $\mathfrak{p}$ of $U_\alpha \cap U_\beta$, it follows that $\phi_{\beta\alpha}(\mathfrak{e})$ is a uniquely determined point on $\pi_\beta^{-1}(U_\alpha \cap U_\beta)$.

From the properties of the family of matrices $\{E^{\beta\alpha}\}_{(\alpha,\beta)\in J\times J}$, we readily obtain the following:

(1) $\phi_{\beta\alpha}$ is a bi-regular mapping from $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$ onto $\pi_\beta^{-1}(U_\alpha \cap U_\beta)$;

(2) $\phi_{\alpha\beta}\phi_{\beta\alpha}$ is the identity map of $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$;

(3) $\phi_{\alpha\gamma}\phi_{\gamma\beta}\phi_{\beta\alpha}$ is the identity map of $\pi_\alpha^{-1}(U_\alpha \cap U_\beta \cap U_\gamma)$;

(4) The restriction of $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$ and $\pi_\beta\phi_{\beta\alpha}$ are equal regular mappings of $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$ onto $U_\alpha \cap U_\beta$. Now for each ordered pair (α, β), identify the open set $\pi_\alpha^{-1}(U_\alpha \cap U_\beta)$ on $U_\alpha \times U_\beta$ with the open set $\pi_\beta^{-1}(U_\alpha \cap U_\beta)$ on $U_\beta \times P_\beta$ according to the rule that $\mathfrak{e}$ and $\phi_{\beta\alpha}(\mathfrak{e})$ are identical. The consistency of this method of identification follows from our previous assertions, and the set of points so obtained is covered by the family of subsets $\{U_\alpha \times P_\alpha\}_{\alpha\in J}$. We equip this set with the structure of an algebraic variety $\mathcal{B}(E)$ such that

1) $\{U_\alpha \times P_\alpha\}$ forms a covering of $\mathcal{B}(E)$ by open sets,

2) The algebro-geometric structure of $U_\alpha \times P_\alpha$ as product variety coincides with the one it inherits as open set on $\mathcal{B}(E)$. We define a regular rational mapping π_E from $\mathcal{B}(E)$ onto X according to the rule that the restriction of π_E to $U_\alpha \times P_\alpha$ is equal to π_α. π_E equips $\mathcal{B}(E)$ with the structure of a projective fibre bundle over X with a projective space of dimension $n-1$ for fiber. Eventually, we shall prove that $\mathcal{B}(E)$ admits a bi-regular mapping onto a projective model.

$\mathcal{B}(E)$ is called the "dual projective bundle" of the sheaf E; it is independent of the particular family of generating sections utilized in its construction. Indeed, let $e'_1, \cdots, e'_n$ be sections of E over an open set U' on X such that $e'_1(\mathfrak{p}), \cdots, e'_n(\mathfrak{p})$ freely generate $E_\mathfrak{p}$ at each point $\mathfrak{p}$ on U'. Let P' be a projective space of dimension $n-1$ and fix a homogeneous coordinate system $\tau'_1, \cdots, \tau'_n$ for P'. Form the product variety $U' \times P'$ and let π' be the coordinate projection from $U' \times P'$ onto U'. We shall construct a bi-regular mapping ϕ' of $U' \times P'$ onto the open set $\pi_E^{-1}(U')$. Now for any $\alpha \in J$,

$$e'_j = \sum_{i=1}^{n} E^\alpha{}_i{}'_j e^\alpha{}_i, \qquad 1 \leqq j \leqq n,$$

where $E^\alpha{}_i{}'_j$ is regular on $U' \cap U_\alpha$ for all $1 \leqq i, j \leqq n$. Furthermore, $\det E^{\alpha\prime}$ is a unit in the local ring of X at any point $\mathfrak{p}$ on $U' \cap U_\alpha$. If $\mathfrak{e}'$ is a point on $(\pi')^{-1}(U' \cap U_\alpha)$, then $\phi'(\mathfrak{e}')$ is that point of $\mathcal{B}(E)$ such that

1) $\pi_E(\phi'(\mathfrak{e}')) = \pi'(\mathfrak{e}') = \mathfrak{p} \in U' \cap U_\alpha$,

2) $\rho_1 \tau'_j(\mathfrak{e}') = \rho_2 \sum_{i=1}^{n} E^\alpha{}_i{}'_j(\mathfrak{p}) \tau^\alpha{}_i(\phi'(\mathfrak{e}')), \qquad 1 \leqq j \leqq n.$

One easily checks that $\phi'(\mathfrak{e}')$ does not depend upon the particular α such that $\mathfrak{e}' \in (\pi')^{-1}(U' \cap U_\alpha)$. We shall say that the sections $(e^\alpha{}_1, \cdots, e^\alpha{}_n)$ are paired with the homogeneous coordinates $\tau^\alpha{}_1, \cdots, \tau^\alpha{}_n$ with reference to the construction of $\mathcal{B}(E)$. The above argument shows that for any generating sections $e'_1, \cdots, e'_n$ of E over U', there are uniquely determined homogeneous coordinates on $\pi_E^{-1}(U')$ which are paired with $e'_1, \cdots, e'_n$ with reference to the construction of $\mathcal{B}(E)$. Furthermore, any different construction of the "dual projective bundle" is in bi-regular correspondence with $\mathcal{B}(E)$ in exactly one way which conserves the pairing of sections and homogeneous coordinates.

§ 4. For any $\alpha \in J$, $1 \leqq i \leqq n$, let $U_{\alpha,i}$ be the open set on $\mathcal{B}(E)$ consisting of all points $\mathfrak{e}$ on $U_\alpha \times P_\alpha$ $(= \pi_E^{-1}(U_\alpha))$ such that $\tau^\alpha{}_i(\mathfrak{e}) \neq 0$. The

family $\{U_{\alpha,i}\}_{\alpha\in J, 1\leqq i\leqq n}$ forms an open covering of $\mathfrak{B}(E)$. For any ordered pair of couples (α,i), (β,j), we set

$$f^{\beta}{}_{j}{}^{\alpha}{}_{i}=\sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{i}\tau^{\beta}{}_{h}/\tau^{\beta}{}_{j}.$$

Observe that $f^{\beta}{}_{j}{}^{\alpha}{}_{i}$ is regular on $U_{\alpha,i}\cap U_{\beta,j}$. We also have that

$$f^{\beta}{}_{j}{}^{\alpha}{}_{i}\tau^{\alpha}{}_{k}/\tau^{\alpha}{}_{i}=\sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{k}\tau^{\beta}{}_{h}/\tau^{\beta}{}_{j}, \qquad 1\leqq k\leqq n, \tag{1}$$

which proves that $f^{\beta}{}_{j}{}^{\alpha}{}_{i}$ vanishes at no point of $U_{\alpha,i}\cap U_{\beta,j}$, and that

$$f^{\alpha}{}_{i}{}^{\gamma}{}_{k}f^{\gamma}{}_{k}{}^{\beta}{}_{j}f^{\beta}{}_{j}{}^{\alpha}{}_{i}=1,$$

$$f^{\alpha}{}_{i}{}^{\beta}{}_{j}f^{\beta}{}_{j}{}^{\alpha}{}_{i}=1.$$

We construct a locally free sheaf $B(E)$ of dimension one defined on $\mathfrak{B}(E)$ as follows. The restriction of $B(E)$ to any $U_{\alpha,i}$ is a free sheaf of dimension one generated by a section $E[\alpha,i]$. On $U_{\alpha,i}\cap U_{\beta,j}$, we have the transition law

$$E[\alpha,i]=f^{\beta}{}_{j}{}^{\alpha}{}_{i}E[\beta,j].$$

Consider the sheaf $\pi_E E$, the reciprocal image of E by π_E, and for notational convenience, set

$$*E=\pi_E E.$$

The restriction of $*E$ to any $U_\alpha\times P_\alpha$ is a free sheaf of dimension n generated by the sections $\pi_E{}^{-1}e^{\alpha}{}_{1},\cdots,\pi_E{}^{-1}e^{\alpha}{}_{n}$ which are the reciprocal images of $e^{\alpha}{}_{1},\cdots,e^{\alpha}{}_{n}$, and we set

$$*e^{\alpha}{}_{i}=\pi_E{}^{-1}e^{\alpha}{}_{i}, \qquad 1\leqq i\leqq n.$$

For each (α,i), let $S_{\alpha,i}$ be the subsheaf of the restriction of $*E$ to $U_{\alpha,i}$ which is generated by the sections

$$*e^{\alpha}{}_{h}-\tau^{\alpha}{}_{h}/\tau^{\alpha}{}_{i}{}^{*}e^{\alpha}{}_{i}, \qquad 1\leqq h\leqq n.$$

$S_{\alpha,i}$ is a free sheaf of dimension $n-1$ defined on $U_{\alpha,i}$. Now

$$*e^{\alpha}{}_{h}=\sum_{j=1}^{n} E^{\beta}{}_{j}{}^{\alpha}{}_{h}{}^{*}e^{\beta}{}_{j}, \qquad 1\leqq h\leqq n,$$

on $\pi_E{}^{-1}(U_\alpha\cap U_\beta)$, which leads to

$$*e^{\alpha}{}_{h}-\tau^{\alpha}{}_{h}/\tau^{\alpha}{}_{i}{}^{*}e^{\alpha}{}_{i}=\sum_{k=1}^{n}(E^{\beta}{}_{k}{}^{\alpha}{}_{h}-E^{\beta}{}_{k}{}^{\alpha}{}_{i}\tau^{\alpha}{}_{h}/\tau^{\alpha}{}_{i}){}^{*}e^{\beta}{}_{k},$$

and making use of (1), we obtain

$$*e^{\alpha}{}_h - \tau^{\alpha}{}_h/\tau^{\alpha}{}_i{}^*e^{\alpha}{}_i = (f^{\beta}{}_j{}^{\alpha}{}_i)^{-1}\sum_{k=1}^{n}\mathcal{E}^{\beta}{}_{ji;}{}^{\alpha}{}_{kh}\,(*e^{\beta}{}_k - \tau^{\beta}{}_k/\tau^{\beta}{}_j{}^*e^{\beta}{}_j),$$

where

$$(2)\quad \mathcal{E}^{\beta}{}_{ji;}{}^{\alpha}{}_{kh} = E^{\beta}{}_k{}^{\alpha}{}_h\Big(\sum_{l=1}^{n}E^{\beta}{}_l{}^{\alpha}{}_i\tau^{\beta}{}_l/\tau^{\beta}{}_j\Big) - E^{\beta}{}_k{}^{\alpha}{}_i\Big(\sum_{l=1}^{n}E^{\beta}{}_l{}^{\alpha}{}_h\tau^{\beta}{}_l/\tau^{\beta}{}_j\Big) = E^{\beta}{}_k{}^{\alpha}{}_h f^{\beta}{}_j{}^{\alpha}{}_i - E^{\beta}{}_k{}^{\alpha}{}_i f^{\beta}{}_j{}^{\alpha}{}_h.$$

We have proved that the restriction of $S_{\alpha,i}$ to $U_{\alpha,i}\cap U_{\beta,j}$ is equal to the restriction of $S_{\beta,j}$ to $U_{\alpha,i}\cap U_{\beta,j}$. Thus we obtain a locally free sheaf δE of dimension $n-1$ defined on $\mathcal{B}(E)$ whose restriction to any $U_{\alpha,i}$ is the sheaf $S_{\alpha,i}$. δE is called the "derived sheaf" of the sheaf E. The sheaf δE is intrinsically associated with E since its restriction $S_{\alpha,i}$ to any $U_{\alpha,i}$ depends upon the pairing of $e^{\alpha}{}_1,\cdots,e^{\alpha}{}_n$ with $\tau^{\alpha}{}_1,\cdots,\tau^{\alpha}{}_n$, which is an intrinsic property of $\mathcal{B}(E)$.

The restriction of $*E$ to any $U_{\alpha,i}$ is a free sheaf of dimension n generated by the sections

$$\begin{aligned}&*e^{\alpha}{}_i,\\ &*e^{\alpha}{}_h - \tau^{\alpha}{}_h/\tau^{\alpha}{}_i{}^*e^{\alpha}{}_i, &\qquad h\neq i,\ 1\leqq h\leqq n.\end{aligned}$$

We construct a homomorphism of $*E$ onto $B(E)$ according to the rule that its restriction to any $U_{\alpha,i}$ is described by

$$\begin{aligned}&*e^{\alpha}{}_i \to E[\alpha,i],\\ &*e^{\alpha}{}_h - (\tau^{\alpha}{}_h/\tau_{\alpha i})*e^{\alpha}{}_i \to 0.\end{aligned}$$

To prove that the homomorphism is properly defined, we observe that

$$\begin{aligned}*e^{\alpha}{}_i &= \sum_{h=1}^{n}E^{\beta}{}_h{}^{\alpha}{}_i{}^*e^{\beta}{}_h\\ &= \Big(\sum_{h=1}^{n}E^{\beta}{}_h{}^{\alpha}{}_i\tau^{\beta}{}_h/\tau^{\beta}{}_j\Big)*e^{\beta}{}_j + \sum_{h=1}^{n}E^{\beta}{}_h{}^{\alpha}{}_i(*e^{\beta}{}_h - \tau^{\beta}{}_h/\tau^{\beta}{}_j{}^*e^{\beta}{}_j)\end{aligned}$$

on $U_{\alpha,i}\cap U_{\beta,j}$, and that

$$E[\alpha,i] = \Big(\sum_{h=1}^{n}E^{\beta}{}_h{}^{\alpha}{}_i\tau^{\beta}{}_h/\tau^{\beta}{}_j\Big)E[\beta,j].$$

The kernel of this homomorphism is the sheaf δE; consequently, we can identify $B(E)$ with the quotient sheaf of $*E$ modulo δE, and, as such, $B(E)$ intrinsically depends upon E and we call $B(E)$ the "basic sheaf" of E. The exact sequence

$$(3)\qquad 0\to\delta E\to\pi_E E\to B(E)\to 0$$

of locally free sheaves defined on $\mathfrak{B}(E)$ is called the "derived sequence" of the sheaf E.

We iterate this process and obtain the derived sheaf of δE which is a locally free sheaf of dimension $n-2$ defined on $\mathfrak{B}(\delta E)$, and which we denote as $\delta_2 E$ and call it the second derived sheaf of E. Thus we have the exact sequence

$$0 \to \delta_2 E \to \pi_{\delta E}\delta E \to B(\delta E) \to 0$$

of locally free sheaves defined on $\mathfrak{B}(\delta E)$. Repeating the process, we obtain for $1 \leqq s \leqq n-1$ the exact sequence

$$0 \to \delta_s E \to \pi_{\delta_{s-1}E}\delta_{s-1}E \to B(\delta_{s-1}E) \to 0 \tag{3'}$$

of locally free sheaves defined on $\mathfrak{B}(\delta_{s-1}E)$. The s-th derived sheaf $\delta_s E$ is a locally free sheaf of dimension $n-s$ defined on $\mathfrak{B}(\delta_{s-1}E)$.

Let ${}^{\#}E$ (resp. ${}^{\#}B(E)$) denote the reciprocal image of E (resp. $B(E)$) with respect to the regular map from $\mathfrak{B}(\delta_{n-2}E)$ onto X (resp. $\mathfrak{B}(E)$) which is the composite map $\pi_E \circ \cdots \circ \pi_{\delta_{n-2}E}$ (resp. $\pi_{\delta_1 E} \circ \cdots \circ \pi_{\delta_{n-2}E}$). Similarly, let ${}^{\#}\delta_s\mathrm{E}$ (resp. ${}^{\#}B(\delta_s E)$) denote the reciprocal image of $\delta_s E$ (resp. $B(\delta_s E)$) with respect to the regular map from $\mathfrak{B}(\delta_{n-2}E)$ onto $\mathfrak{B}(\delta_{s-1}E)$ (resp. $\mathfrak{B}(\delta_s E)$). ${}^{\#}E$ is a locally free sheaf of dimension n defined on $\mathfrak{B}(\delta_{n-2}E)$ and it has a composition series

$${}^{\#}E \supset {}^{\#}\delta_1 E \supset \cdots \supset {}^{\#}\delta_{n-1}E = \delta_{n-1}E. \tag{4}$$

${}^{\#}\delta_s E$ is a locally free sheaf of dimension $n-s$ defined on $\mathfrak{B}(\delta_{n-2}E)$ and the quotient sheaf ${}^{\#}\delta_s E/{}^{\#}\delta_{s-1}E$ is canonically isomorphic with ${}^{\#}B(\delta_s E)$.

§ 5. For $2 \leqq s \leqq n$, we form the sheaf $\wedge^s E$ which is the exterior product of E taken s times, and we set $\wedge^1 E = E$. $\wedge^s E$ is a locally free sheaf of dimension $n!/s!(n-s)!$ defined on X. The stalk $\wedge^s E_{\mathfrak{p}}$ at any point $\mathfrak{p} \in U_\alpha$ is the exterior product of $E_{\mathfrak{p}}$ taken s times and its is freely generated by

$$e^\alpha{}_{h_1}(\mathfrak{p}) \wedge \cdots \wedge e^\alpha{}_{h_s}(\mathfrak{p}), \qquad 1 \leqq h_1 < \cdots < h_s \leqq n.$$

We set

$$e^\alpha{}_{h_1\cdots h_s}(\mathfrak{p}) = e^\alpha{}_{h_1}(\mathfrak{p}) \wedge \cdots \wedge e^\alpha{}_{h_s}(\mathfrak{p})$$

and agree that $e^\alpha{}_{h_1\cdots h_s}(\mathfrak{p})$ is defined for all sequences of s integers from $\{1, \cdots, n\}$ but that it is strictly skew-symmetric in its subscripts (hence zero if two subscripts are equal). The restriction of $\wedge^s E$ to any U_α is a free sheaf generated (freely) by sections

$$e^\alpha{}_{h_1\cdots h_s}, \qquad 1 \leqq h_1 < \cdots < h_s \leqq n,$$

where the image of $e^\alpha{}_{h_1\cdots h_s}$ in $(\wedge^s E)_{\mathfrak{p}}$ is $e^\alpha{}_{h_1\cdots h_s}(\mathfrak{p})$.

Consider the reciprocal image $\pi_E \wedge^s E$ of $\wedge^s E$ with respect to π_E and set

$$*E^s = \pi_E \wedge^s E.$$

The restriction of $*E^s$ to any $U_\alpha \times P_\alpha$ is a free sheaf of dimension $n!/s!(n-s)!$ generated by the sections

$$*e^\alpha_{h_1\cdots h_s}, \qquad 1 \leqq h_1 < \cdots < h_s \leqq n,$$

where $*e^\alpha_{h_1\cdots h_s}$ is the reciprocal image of $e^\alpha_{h_1\cdots h_s}$. From our canonical isomorphism of δE into $*E$, we construct a canonical isomorphism of $\wedge^s(\delta E)$ into $\wedge^s(*E) = *E^s = \pi_E \wedge^s E$. For the restriction of δE to any U_{α,h_0} is a free sheaf generated by the sections

$$*e^\alpha_h - (\tau^\alpha_h/\tau^\alpha_{h_0}) *e^\alpha_{h_0}, \qquad h \neq h_0, 1 \leqq h \leqq n;$$

hence the restriction of $\wedge^s(\delta E)$ to U_{α,h_0} is a free sheaf of dimension $(n-1)!/s!(n-1-s)!$ generated by the sections

$$(*e^\alpha_{h_1} - (\tau^\alpha_{h_1}/\tau^\alpha_{h_0}) *e^\alpha_{h_0}) \wedge \cdots \wedge (*e^\alpha_{h_s} - (\tau^\alpha_{h_s}/\tau^\alpha_{h_0}) *e^\alpha_{h_0})$$

for all $1 \leqq h_1 < \cdots < h_s \leqq n$ for all $1 \leqq i \leqq s$. The isomorphism from $\wedge^s(\delta E)$ into $\wedge^s(*E)$ is defined according to the rule that its restriction to U_{α,h_0} is given by

$$(*e^\alpha_{h_1} - \tau^\alpha_{h_1}/\tau^\alpha_{h_0} *e^\alpha_{h_0}) \wedge \cdots \wedge (*e^\alpha_{h_s} - \tau^\alpha_{h_s}/\tau^\alpha_{h_0} *e^\alpha_{h_0}) \rightarrow$$

$$*e^\alpha_{h_1\cdots h_s} + \sum_{p=1}^{s} (-1)^p (\tau^\alpha_{h_p}/\tau^\alpha_{h_0}) *e^\alpha_{h_0 h_1\cdots \hat{h}_p \cdots h_s}.$$

($*e^\alpha_{h_0 h_1\cdots \hat{h}_p \cdots h_s}$ is obtained by suppressing the index h_p from the sequence of $s+1$ interegers $h_0, \cdots, h_s$.) Indeed, the restriction of $\wedge^s(*E)$ to U_{α,h_0} is freely generated by the sections

$$*e^\alpha_{h_0 k_1\cdots k_{s-1}}, \qquad 1 \leqq k_1 < \cdots < k_{s-1} \leqq n, k_i \neq h_0,$$

$$*e^\alpha_{h_1\cdots h_s} + \sum_{p=1}^{s} (-1)^p (\tau^\alpha_{h_p}/\tau^\alpha_{h_0}) *e^\alpha_{h_0 h_1\cdots \hat{h}_p \cdots h_s},$$
$$1 \leqq h_1 < \cdots < h_s \leqq n, h_i \neq h_0,$$

and we can view $\wedge^s(\delta E)$ as a subsheaf $\wedge^s(*E)$.

It is evident that the quotient sheaf of $\wedge^s(*E)$ modulo $\wedge^s(\delta E)$ is a locally free sheaf defined on $\mathfrak{B}(E)$. We shall construct a canonical isomorphism of this quotient sheaf into the tensor product sheaf $\wedge^{s-1}(*E) \otimes B(E)$. For the restriction of $\wedge^{s-1}(*E) \otimes B(E)$ to U_{α,h_0} is a free sheaf generated by

$$*e^\alpha_{h_0 k_1\cdots k_{s-2}} \otimes E[\alpha, h_0], \qquad 1 \leqq k_1 < \cdots < k_{s-2} \leqq n, k_i \neq h_0,$$

$$*e_{k_1\cdots k_{s-1}} \otimes E[\alpha, h_0] - \sum_{p=1}^{s-1} (-1)^p (\tau^\alpha_{h_p}/\tau^\alpha_{h_0}) *e_{h_0 k_1 \cdots \hat{k}_p \cdots k_{s-1}} \otimes E[\alpha, h_0]$$

for all $1 \leqq k_1 < \cdots < k_{s-1} \leqq n-1$, $k_i \neq h_0$. We construct a homomorphism from $\wedge^s(^*E)$ into $\wedge^{s-1}(^*E) \otimes B(E)$ according to the rule that its restriction to U_{α,h_0} is given by

$$e_{h_1\cdots h_s} \rightarrow \sum_{p=1}^{s} (-1)^{p-1} (\tau^{\alpha}{}_{h_p}/\tau^{\alpha}{}_{h_0})^* e^{\alpha}{}_{h_1\cdots \hat{h}_p \cdots h_s} \otimes E[\alpha, h\ ].$$

One checks that we have properly defined a homomorphism, that its kernel is $\wedge^s(\delta E)$, and that the image of $\wedge^s(^*E)$ is $\wedge^{s-1}(\delta E) \otimes B(E)$. Thus we have the exact sequence

$$(5) \qquad 0 \rightarrow \wedge^s(\delta E) \rightarrow \wedge^s(^*E) \rightarrow \wedge^{s-1}(\delta E) \otimes B(E) \rightarrow 0,$$

which specializes to the derived sequence

$$0 \rightarrow \delta E \rightarrow {}^*E \rightarrow B(E) \rightarrow 0$$

for $s = 1$.

Let $B^{-1}(E)$ be the reciprocal sheaf of $B(E)$. $B^{-1}(E)$ is a locally free sheaf of dimension one defined on $\mathfrak{B}(E)$. The restriction of $B^{-1}(E)$ to any $U_{\alpha,i}$ is a free sheaf of dimension one generated by a section $E^{-1}[\alpha, i]$ over $U_{\alpha,i}$, and we have the transition law

$$E^{-1}[\alpha, i] = (f^{\beta}{}_j{}^{\alpha}{}_i)^{-1} E^{-1}[\beta, j]$$

on $U_{\alpha,i} \cap U_{\beta,j}$, where $f^{\beta}{}_j{}^{\alpha}{}_i$ is, as before, equal to

$$\sum_{h=1}^{n} E^{\beta}{}_h{}^{\alpha}{}_i \tau^{\beta}{}_h / \tau^{\beta}{}_j.$$

The tensor product

$$B^{-1}(E) \otimes B(E)$$

is canonically isomorphic to the sheaf $\mathcal{O}_{\mathfrak{B}(E)}$ of local rings on $\mathfrak{B}(E)$, since we have

$$E[\alpha, i] = f^{\beta}{}_j{}^{\alpha}{}_i E[\beta, j]$$

on any $U_{\alpha,i} \cap U_{\beta,j}$. Taking tensor products with the sheaf $B^{-1}(E)$ a suitable number of times, the previous exact sequences (5) can be merged into a single exact sequence

$$(6) \qquad 0 \rightarrow \wedge^n(^*E \otimes B^{-1}(E)) \rightarrow \cdots \rightarrow \wedge^s(^*E \otimes B^{-1}(E)) \rightarrow \cdots \rightarrow \mathcal{O}_{\mathfrak{B}(E)} \rightarrow 0$$

of locally free sheaves defined on $\mathfrak{B}(E)$. The kernel of

$$\wedge^s(^*E \otimes B^{-1}(E)) \rightarrow \wedge^{s-1}(^*E \otimes B^{-1}(E))$$

is the sheaf

$$\wedge^s(\delta E \otimes B^{-1}(E)).$$

Set

$$B^{-k}(E) = \underbrace{B^{-1}(E) \otimes \cdots \otimes B^{-1}(E)}_{k\text{-times}}.$$

Then we have the exact sequence

$$(7) \quad 0 \to \wedge^n(^*E) \otimes B^{-(n-s)}(E) \to \cdots \to \wedge^{s+k}(^*E) \otimes B^{-k}(E) \to \cdots$$
$$\cdots \to \wedge^{s+1}(^*E) \otimes B^{-1}(E) \to \wedge^s(\delta E) \to 0.$$

Let $\Omega^1{}_X$ denote the sheaf of germs of regular differentials of degree one on X, and similarly we have $\Omega^1{}_{\mathcal{B}(E)}$. Set $^*\Omega^1{}_X$ equal to the sheaf $\pi_E\Omega^1{}_X$, the reciprocal image of $\Omega^1{}_X$ with respect to π_E. Then there is a canonical isomorphism of $^*\Omega^1{}_X$ into $\Omega^1{}_{\mathcal{B}(E)}$, and the quotient sheaf is easily seen to be isomorphic to the sheaf $\delta E \otimes B^{-1}(E)$. Thus we have the exact sequence

$$(8) \qquad 0 \to \pi_E\Omega^1{}_X \to \Omega^1{}_{\mathcal{B}(E)} \to \delta E \otimes B^{-1}(E) \to 0.$$

§ 6. Let z be a rational function on $\mathcal{B}(E)$ with the property that z is regular on some $U_\alpha \times P_\alpha$. We shall prove that z is the reciprocal image of a regular function on U_α. For z is expressible as a quotient P/Q where P, Q are homogeneous polynomials, of equal degree of homogeneity say s, in $\tau^\alpha{}_1, \cdots, \tau^\alpha{}_n$ with coefficients in the field of rational functions on X. We can suppose that P, Q are relatively prime polynomials in $\tau^\alpha{}_1, \cdots, \tau^\alpha{}_n$, and, since U_α is an affine model, we can suppose that the coefficients of P and Q are the reciprocal images of regular functions on U_α. If $s > 0$, then we can find a point $\mathfrak{e}$ on $U_\alpha \times P_\alpha$ such that $P(\mathfrak{e}) \neq 0$ and $Q(\mathfrak{e}) = 0$ since P and Q are relatively prime. Consequently, our assumption that z is regular on $U_\alpha \times P_\alpha$ forces $s = 0$ so that z is then the reciprocal image of a regular function on U_α.

It now follows that the canonical homomorphism from $\Gamma(E, U_\alpha)$ into $\Gamma(\pi_E E, U_\alpha \times P_\alpha)$ is an isomorphism of the former onto the latter. The restriction to $U_{\alpha,i}$ of the homomorphism from $\Gamma(\pi_E E, U_\alpha \times P_\alpha)$ into $\Gamma(B(E), U_\alpha \times P_\alpha)$ is described by

$$\pi_E{}^{-1}e^\alpha{}_h \to (\tau^\alpha{}_h/\tau^\alpha{}_i)E[\alpha, i], \qquad 1 \leq h \leq n.$$

This induces a homomorphism from $\Gamma(E, U_\alpha)$ into $\Gamma(B(E), U_\alpha \times P_\alpha)$ which sends the section

$$c_1 e^\alpha{}_1 + \cdots + c_n e^\alpha{}_n$$

($c_1, \cdots, c_n$ regular on U_α) into the section of $B(E)$ over $U_\alpha \times P_\alpha$ whose restriction to any $U_{\alpha,i}$ is the section

$$\left(\sum_{h=1}^{n} c_h\, \tau^\alpha{}_h/\tau^\alpha{}_i\right)E[\alpha, i].$$

This homomorphism is an isomorphism from $\Gamma(E, U_\alpha)$ into $\Gamma(B(E), U_\alpha \times P_\alpha)$. For $B(E)$ is a locally free sheaf, and if the image section is zero, then

$$\sum_{h=1}^{n} c_h \tau^\alpha{}_h/\tau^\alpha{}_i$$

is the rational function zero. But $\tau^\alpha{}_h/\tau^\alpha{}_i$, $1 \leqq h \leqq n$, $h \neq i$, are $n-1$ algebraically independent functions over the field of rational functions on X which forces $c_1, \cdots, c_n$ equal to zero.

We shall strengthen the last remark by proving that $\Gamma(E, U_\alpha)$ is mapped isomorphically onto $\Gamma(B(E), U_\alpha \times P_\alpha)$. Let σ be a section of $\Gamma(B(E), U_\alpha \times P_\alpha)$. The restriction of σ to any $U_{\alpha,i}$ is equal to

$$z_i E[\alpha, i],$$

where z_i is a regular function on $U_{\alpha,i}$. On $U_{\alpha,i} \cap U_{\alpha,j}$, we have

$$z_i(\tau^\alpha{}_i/\tau^\alpha{}_j) = z_j$$

since

$$E[\alpha, i] = (\tau^\alpha{}_i/\tau^\alpha{}_j) E[\alpha, j],$$

and z_j is regular on $U_{\alpha,j}$. For i fixed, we have

$$z_i = P/Q,$$

where P, Q are homogeneous polynomials, of equal degree of homogeneity s, in $\tau^\alpha{}_1, \cdots, \tau^\alpha{}_n$; the coefficients are regular functions on U_α and P, Q are relatively prime as polynomials over the field of rational functions on X. Now z_i is regular on $U_{\alpha,i}$ which forces Q to be a monomial

$$A(\tau^\alpha{}_i)^s,$$

where A is regular on U. Otherwise, since P and Q are relatively prime, there would exist a point $\mathfrak{e}$ on $U_{\alpha,i}$ such that $Q(\mathfrak{e}) = 0$ and $P(\mathfrak{e}) \neq 0$, which contradicts the assumption that z_i is regular. Choose $j \neq i$ (there is nothing to prove if $n = 1$) and observe that

$$z_j = (\tau^\alpha{}_i/\tau^\alpha{}_j) P/Q = P/A\tau^\alpha{}_j(\tau^\alpha{}_i)^{s-1}$$

is regular on $U_{\alpha,j}$. Since $\tau^\alpha{}_i$ does not divide P, the only possibilities are $s = 0$ or $s = 1$. If $s = 0$, then z_i is the reciprocal image of a regular function z_i on U_α and σ is the image of the section $z_i e^\alpha{}_i$. If $s = 1$, then

$$z_i = \sum_{h=1}^{n} c_h(\tau^\alpha{}_h/\tau^\alpha{}_i),$$

where $c_1, \cdots, c_n$ are regular on U_α and σ is the image of the section

$$\sum_{h=1}^{n} c_h e^\alpha{}_h.$$

Since $E, \pi_B E$, and $B(E)$ are locally free sheaves it follows that $\Gamma(E, X)$, $\Gamma(\pi_B E, \mathfrak{B}(E))$ and $\Gamma(B(E), \mathfrak{B}(E))$ are isomorphic. J. H. Sampson and the author have generalized this result by proving that cohomology modules $H^q(X, E)$, $H^q(\mathfrak{B}(E), \pi_B E)$, and $H^q(\mathfrak{B}(E), B(E))$ are isomorphic for all q.

§ 7. We shall borrow Andre Weil's construction of the basic characteristic class of a locally free sheaf of dimension one. We choose a family $\{g^\alpha{}_i\}$ of rational functions on $\mathfrak{B}(E)$, a function $g^\alpha{}_i$ for each (α, i), such that

1) $g^\alpha{}_i$ is not the function zero for each (α, i),
2) $f^\beta{}_j{}^\alpha{}_i g^\alpha{}_i = g^\beta{}_j$ for each (α, i), (β, j), where

$$f^\beta{}_j{}^\alpha{}_i = \sum_{h=1}^{n} E^\beta{}_h{}^\alpha{}_i (\tau^\beta{}_h / \tau^\beta{}_j).$$

Let W be a proper subvariety on $\mathfrak{B}(E)$ of highest possible dimension (i.e., if $\dim. X = r$, then $\dim. \mathfrak{B}(E) = r + n - 1$ and $\dim. W = r + n - 2$). Choose (α, i) such that the frontier of $U_{\alpha,i}$ does not contain W and define

$$\mathrm{ord}_W \{g\}$$

to be $\mathrm{ord}_W g^\alpha{}_i$, the order of the function $g^\alpha{}_i$ along W; there is no difficulty since $\mathfrak{B}(E)$ is a non-singular variety. Since $f^\beta{}_j{}^\alpha{}_i$ is regular and vanishes at no point of $U_{\alpha,i} \cap U_{\beta,j}$, it follows that

$$\mathrm{ord}_W g^\beta{}_j = \mathrm{ord}_W g^\alpha{}_i$$

if the frontier of $U_{\beta,j}$ does not contain W, so that $\mathrm{ord}_W \{g\}$ is well defined. Let $\vartheta_{\{g\}}$ be the divisor on $\mathfrak{B}(E)$ with

$$\vartheta_{\{g\}} = \sum{}_W (\mathrm{ord}_W \{g\}) W,$$

where the sum is taken over all proper subvarieties W on $\mathfrak{B}(E)$ of highest possible dimension; there are, of course, only finitely many W such that $\mathrm{ord}_W \{g\} \neq 0$. Let $\{h^\alpha{}_i\}$ be some other family with the properties 1) and 2) above. Then there is a unique rational function f on $\mathfrak{B}(E)$, not the function zero, such that

$$f = g^\alpha{}_i / h^\alpha{}_i$$

for each (α, i), since $g^\alpha{}_i / h^\alpha{}_i = g^\alpha{}_j / h^\alpha{}_j$. The divisors $\vartheta_{\{g\}}$ and $\vartheta_{\{h\}}$ are linearly equivalent divisors on $\mathfrak{B}(E)$ and let $\Theta(E)$ denote the common divisor class of these divisors. $\Theta(E)$ is called the "basic divisor class" of the sheaf E. The basic sheaf $B(E)$ is isomorphic with the sheaf $\mathcal{L}(-\vartheta)$ of germs of rational functions on $\mathfrak{B}(E)$ which are multiples of the divisor $-\vartheta$ where ϑ is any divisor of the class $\Theta(E)$. Consequently, we have that

$$B(E) = \mathcal{O}_{\mathfrak{B}(E)}(\Theta(E)).$$

The divisor $\vartheta_{\{g\}}$ is non-negative if and only if $g^{\alpha}{}_{i}$ is a regular function on $U_{\alpha,i}$ for every (α, i). In this situation, we obtain a non-zero element of the module $\Gamma(B(E), \mathcal{B}(E))$. It is the global section of $B(E)$ whose restriction to any $U_{\alpha,i}$ is $g^{\alpha}{}_{i}E[\alpha, i]$. Reciprocally, to each non-zero global section of $B(E)$, there corresponds a unique non-negative divisor of the class $\Theta(E)$, and two non-zero sections of $B(E)$ correspond to the same divisor if and only if they are linearly dependent elements of $\Gamma(B(E), \mathcal{B}(E))$ as vector space over the constant field. In view of the previous isomorphism of $\Gamma(E, X)$ onto $\Gamma(B(E), \mathcal{B}(E))$, it follows that to each non-zero element of $\Gamma(E, X)$, there corresponds a unique non-negative divisor of $\Theta(E)$. If $\dim. \Gamma(E, X) > 0$, then $\Theta(E)$ contains positive divisors except for the case where E is equal to $\mathcal{O}_X$, for here $\Theta(\mathcal{O}_X)$ is the divisor class zero.

§8. Let D be a locally free sheaf of dimension one defined on X. It follows from our constructions that

$$\mathcal{B}(D) = X,$$

and that

$$B(D) = D.$$

We can suppose that the previous covering $\{U_{\alpha}\}$ has the property that the restriction of D to any U_{α} is a free sheaf generated by a section d^{α}. On $U_{\alpha} \cap U_{\beta}$ we have the transition law

$$d^{\alpha} = D^{\beta\alpha} d^{\beta},$$

where $D^{\beta\alpha}$ is regular and vanishes at no point of $U_{\alpha} \cap U_{\beta}$. Form the product cheaf $E \otimes D$. The restriction of $E \otimes D$ to any U_{α} is a free sheaf of dimension n generated by the sections

$$e^{\alpha}{}_{1} \otimes d^{\alpha}, \cdots, e^{\alpha}{}_{n} \otimes d.$$

On $U_{\alpha} \cap U_{\beta}$, wehave the transition laws

$$e^{\alpha}{}_{j} \otimes d^{\alpha} = D^{\beta\alpha} \sum_{i=1}^{n} E^{\beta}{}_{i}{}^{\alpha}{}_{j} e^{\beta}{}_{i} \otimes d^{\beta}, \qquad 1 \leqq i \leqq n.$$

There is an evident bi-regular mapping of $\mathcal{B}(E \otimes D)$ onto $\mathcal{B}(E)$ with the property that $\tau^{\alpha}{}_{1}, \cdots, \tau^{\alpha}{}_{n}$ corresponds to the homogeneous coordinate system paired with $e^{\alpha}{}_{1} \otimes d^{\alpha}, \cdots, e^{\alpha}{}_{n} \otimes d^{\alpha}$ for every $\alpha \in J$. Thus

$$\mathcal{B}(E \otimes D) = \mathcal{B}(E)$$

and

$$B(E \otimes D) = B(E) \otimes_{\pi_E} D.$$

We also have that

$$\Theta(E \otimes D) = \Theta(E) + \pi_E{}^{*}\Theta(D),$$

where $\pi_E{}^*\Theta(D)$ is the reciprocal image of the divisor class $\Theta(D)$ with respect to π_E.

Let Y be a non-singular projective model, and let Φ be a regular mapping from Y into X. $\mathcal{B}(\Phi E)$, the dual projective bundle of the reciprocal image sheaf ΦE, is identical to the induced bundle of $\mathcal{B}(E)$ by the mapping Φ. Furthermore, $B(\Phi E)$ is the reciprocal image of $B(E)$ by the fiber mapping of $\mathcal{B}(\Phi E)$ into $\mathcal{B}(E)$ which covers the mapping Φ of Y into X, and $\Theta(\Phi E)$ is the divisor class on $\mathcal{B}(\Phi E)$ which is the reciprocal image of $\Theta(E)$ by that fiber mapping.

§ 9. Let V be a non-singular subvariety of dimension d on the non-singular projective model X of dimension r. Consider the sheaf $\mathfrak{J}(X;V)$ of ideals determined by V on X; the stalk of $\mathfrak{J}(X;V)$ at any point $\mathfrak{p}$ on X is the ideal determined by V in the local ring $\mathcal{O}_{\mathfrak{p}}$ of X at $\mathfrak{p}$. The induced sheaf of $\mathfrak{J}(X;V)$ on the subvariety V (i.e., the reciprocal image with respect to the identity map of V into X) is a locally free sheaf $N(X;V)$ of dimension $r-d$ defined on V which we call the sheaf of covariant normal vectors to V on X.

To prove the above assertions, we choose a covering $\mathfrak{U}=\{U_\alpha\}_{\alpha\in J}$ of X consisting of finitely many non-empty open set U_α such that each U_α admits a biregular correspondence onto an affine model and with the following additional properties:

1) If $U_\alpha\cap V$ is non-empty, then there exist $r-d$ regular functions $x^\alpha{}_1,\cdots,x^\alpha{}_{r-d}$ on U_α which generate the ideal determined by V in the local ring of X at any point on U_α;

2) For each point $\mathfrak{p}$ on U_α, the $r-d$ functions $x^\alpha{}_h-x^\alpha{}_h(\mathfrak{p})$, $1\leqq h\leqq r-d$, ($x^\alpha{}_h(\mathfrak{p})$ is the value of $x_{\alpha h}$ at $\mathfrak{p}$) can be extended to a basis of $r-d$ elements for the maximal prime ideal in the local ring of X at $\mathfrak{p}$;

3) Each $U_\alpha\cap U_\beta$ admits a bi-regular mapping onto an affine model. The possibility of choosing such a covering follows from the assumption that X and V are non-singular together with the quasi-compactness of the Zariski topology.

Let J^* be the subset of J consisting of those α such that $U_\alpha\cap V$ is non-empty. Given $\alpha,\beta\in J^*$, it is possible to choose regular functions $N^\beta{}_g{}^\alpha{}_h$, $1\leqq g,h\leqq r-d$, on $U_\alpha\cap U_\beta$ such that

$$x^\alpha{}_h=\sum_{g=1}^{r-d}N^\beta{}_g{}^\alpha{}_h x^\beta{}_g, \qquad 1\leqq h\leqq r-d,$$

for the restrictions of $x^{\alpha}_1, \cdots, x^{\alpha}_{r-d}$ to $U_\alpha \cap U_\beta$ generate the module of sections of $\mathfrak{J}(X;V)$ over $U_\alpha \cap U_\beta$ since that open set is an affine model. If $r-d>1$, then the $N^{\beta}{}_{g}{}^{\alpha}{}_{h}$ are not uniquely determined by the choice of the families $\{x^{\alpha}_1, \cdots, x^{\alpha}_{r-d}\}_{\alpha \in J^*}$; however, their induced functions on V, which we continue to denote as $N^{\beta}{}_{g}{}^{\alpha}{}_{h}$, are regular functions on $U_\alpha \cap U_\beta \cap V$ which are uniquely determined by the families $\{x^{\alpha}_1, \cdots, x^{\alpha}_{r-d}\}_{\alpha \in J^*}$.

Let $\mathfrak{p}$ be any point on V; say that $\mathfrak{p} \in U_\alpha \cap V$. The stalk $\mathfrak{J}(X;V)_{\mathfrak{p}}$ is the submodule of $\mathcal{O}_{\mathfrak{p}}$ generated by $x^{\alpha}_1, \cdots, x^{\alpha}_{r-d}$. Let $\mathcal{O}(V,\mathfrak{p})$ denote the local ring of V at $\mathfrak{p}$; it is the residue class ring of $\mathcal{O}_{\mathfrak{p}}$ modulo the ideal $\mathfrak{J}(X;V)_{\mathfrak{p}}$ so that $\mathcal{O}(V;\mathfrak{p})$ carries the structure of an $\mathcal{O}_{\mathfrak{p}}$-module. Form the tensor product $\mathcal{O}(V;\mathfrak{p}) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathfrak{J}(X;V)_{\mathfrak{p}}$; it is the stalk $N(X;V)_{\mathfrak{p}}$ with the structure of an $\mathcal{O}_{\mathfrak{p}}$-module. We have that

$$1 \otimes x^{\alpha}_1, \cdots, 1 \otimes x^{\alpha}_{r-d}, \qquad 1 \in \mathcal{O}(V;\mathfrak{p}),$$

generate $N(X;V)_{\mathfrak{p}}$ as $\mathcal{O}(V,\mathfrak{p})$-module. Set

$$z^{\alpha}_h = 1 \otimes x^{\alpha}_h, \qquad 1 \leqq h \leqq r-d;$$

then we shall prove that $N(X;V)_{\mathfrak{p}}$ is the free $\mathcal{O}(V;\mathfrak{p})$-module generated by $z^{\alpha}_1, \cdots, z^{\alpha}_{r-d}$. Let F be a free $\mathcal{O}_{\mathfrak{p}}$-module of dimension $r-d$ with generators $f_1, \cdots, f_{r-d}$, and define a homomorphism from F onto $\mathfrak{J}(X;V)_{\mathfrak{p}}$ according to

$$f_h \to x^{\alpha}_h, \qquad 1 \leqq h \leqq r-d.$$

The kernel of this homomorphism is the submodule R of F generated by

$$x^{\alpha}_{h_1} f_{h_2} - x^{\alpha}_{h_2} f_{h_1}, \qquad 1 \leqq h_1 < h_2 \leqq r-d,$$

since $\mathfrak{p}$ is a simple point on V. From the exact sequence

$$0 \to R \to F \to \mathfrak{J}(X,V)_{\mathfrak{p}} \to 0$$

of $\mathcal{O}_{\mathfrak{p}}$-modules, we pass to the exact sequence of $\mathcal{O}(V;\mathfrak{p})$-modules

$$\mathcal{O}(V;\mathfrak{p}) \otimes R \to \mathcal{O}(V;\mathfrak{p}) \otimes F \to N(X;V)_{\mathfrak{p}} \to 0$$

which is obtained by tensorizing with $\mathcal{O}(V;\mathfrak{p})$ viewed as $\mathcal{O}_{\mathfrak{p}}$-module, and then viewing each module as $\mathcal{O}(V;\mathfrak{p})$-module. We have that $\mathcal{O}(V;\mathfrak{p}) \otimes F$ is a free $\mathcal{O}(V;\mathfrak{p})$-module generated by

$$1 \otimes f_h, \qquad 1 \leqq h \leqq r-d,$$

and that the homomorphism

$$\mathcal{O}(V;\mathfrak{p}) \otimes R \to \mathcal{O}(V;\mathfrak{p}) \otimes F$$

maps the first module onto the zero module since it sends each element

$$1 \otimes (x^\alpha{}_{h_1} f_{h_2} - x^\alpha{}_{h_2} f_{h_1}), \qquad 1 \leqq h_1 < h_2 \leqq r - d,$$

of $\mathcal{O}(V;\mathfrak{p}) \otimes R$ onto the element

$$x^\alpha{}_{h_1} \otimes f_{h_2} - x^\alpha{}_{h_2} \otimes f_{h_1} = 0$$

of $\mathcal{O}(V;\mathfrak{p}) \otimes F$. Consequently, we have the exact sequence

$$0 \to \mathcal{O}(V;\mathfrak{p}) \otimes F \to N(X;V)_{\mathfrak{p}} \to 0,$$

with

$$1 \otimes f_h \to z^\alpha{}_h, \qquad 1 - h - r - d;$$

and this proves that $N(X;V)$ is a locally free sheaf of dimension $r-d$ defined on V.

Thus the restriction of $N(X;V)$ to any $U_\alpha \cap V$ is a free sheaf dimension $r-d$ generated by sections

$$z^\alpha{}_h = 1 \otimes x^\alpha{}_h, \qquad 1 \leqq h \leqq r - d,$$

(where 1 is the section 1 of $\mathcal{O}_V$ over $U_\alpha \cap V$), and we have the transition laws

$$z^\alpha{}_h = \sum_{g=1}^{r-d} N^\beta{}_g{}^\alpha{}_h z^\beta{}_g, \qquad 1 \leqq h \leqq r - d,$$

on any $U_\alpha \cap U_\beta \cap V$.

The sheaf $N(X;V)$ depends solely upon the embedding of V in X; it is essentially the sheaf of germs of cross sections of the vector bundle of differentials on X which are normal to the subvariety V (i.e., the dual space to the subspace of tangent vectors of V in the tangent space of X). We also have the exact sequence

$$0 \to N(X;V) \to (\Omega^1{}_X)' \to \Omega^1{}_V \to 0$$

of locally free sheaves defined on V. $(\Omega^1{}_X)'$ is the induced sheaf on V of the sheaf of differentials of degree one on X; and $\Omega^1{}_V$ is the sheaf of differentials of degree one on V.

§ 10. We shall review the classical construction of the variety X^* which is obtained from monoidal transformation of X centered on V; it is related to the construction of the sheaf $N(X;V)$ in § 9. Choose a projective space $P^*{}_\alpha$ of dimension $r-d-1$ for each $\alpha \in J^*$ and fix a homogeneous coordinate system $\zeta^\alpha{}_1, \cdots, \zeta^\alpha{}_{r-d}$ on $P^*{}_\alpha$. Form the product variety $U_\alpha \times P^*{}_\alpha$ and let $U^*{}_\alpha$ denote the set of all points $\mathfrak{p}^*$ on $U_\alpha \times P^*{}_\alpha$ such that

$$x^\alpha{}_{h_1}(\mathfrak{p}^*)\zeta^\alpha{}_{h_2}(\mathfrak{p}^*) - x^\alpha{}_{h_2}(\mathfrak{p}^*)\zeta^\alpha{}_{h_1}(\mathfrak{p}^*) = 0$$

for all $1 \leqq h_1, h_2 \leqq r-d$. U^*_α is a non-singular subvariety of dimension r on $U_\alpha \times P^*_\alpha$. Let $\mathfrak{p}^*$ be any point on U^*_α, and say that $\zeta^\alpha_{h_0}(\mathfrak{p}^*) \neq 0$ for some h_0, $1 \leqq h_0 \leqq r-d$. Then the $r-d-1$ functions.

$$x^\alpha_h - x^\alpha_{h_0}(\zeta^\alpha_h/\zeta^\alpha_{h_0}), \qquad 1 \leqq h \leqq r-d, h \neq h_0,$$

generate the ideal determined by U^*_α in the local ring of $U_\alpha \times P^*_\alpha$ at $\mathfrak{p}^*$; this proves that U^*_α is a non-singular subvariety of dimension r on $U_\alpha \times P^*_\alpha$.

Let Φ_α denote the restriction to U^*_α of the coordinate projection from $U_\alpha \times P^*_\alpha$ onto U_α. Φ_α is a regular mapping from U^*_α onto U_α. If a point $\mathfrak{p}$ on U_α is not on V, then there is one and only one point $\mathfrak{p}^*$ on U^*_α such that $\Phi_\alpha(\mathfrak{p}^*) = \mathfrak{p}$, and Φ_α bi-regularly maps some open neighborhood of $\mathfrak{p}^*$ on U^*_α onto an open neighborhood of $\mathfrak{p}$ on U_α.

If $\mathfrak{p} \in U_\alpha \cap V$, then $\Phi_\alpha^{-1}(\mathfrak{p})$ is a non-singular subvariety on U^*_α and it is in bi-regular correspondence with a projective space of dimension $r-d-1$; in fact, $\Phi_\alpha^{-1}(\mathfrak{p}) = (\mathfrak{p}) \times P^*_\alpha$. Furthermore, $V^*_\alpha = \Phi_\alpha^{-1}(U_\alpha \cap V)$ is a non-singular subvariety of dimension $r-1$ on U^*_α and it is in bi-regular correspondence with the product variety $(U_\alpha \cap V) \times P^*_\alpha$. Let $U^*_{\alpha,h}$ denote the open set on U^*_α consisting of all points $\mathfrak{p}^*$ which satisfy $\zeta^\alpha_h(\mathfrak{p}^*) \neq 0$. Then the function x^α_h generates the ideal determined by V^*_α in the local ring of U^*_α at every point on $U^*_{\alpha,h}$.

We construct a bi-regular mapping $\eta_{\beta\alpha}$ from $\Phi_\alpha^{-1}(U_\alpha \cap U_\beta)$ onto $\Phi_\beta^{-1}(U_\alpha \cap U_\beta)$ for each $\alpha, \beta \in J^*$ as follows: for $\mathfrak{p}^* \in \Phi_\alpha^{-1}(U_\alpha \cap U_\beta)$, $\eta_{\beta\alpha}(\mathfrak{p}^*)$ is that point on $\Phi_\beta^{-1}(U_\alpha \cap U_\beta)$ such that

1) $\Phi_\beta(\eta_{\beta\alpha}(\mathfrak{p}^*)) = \Phi_\alpha(\mathfrak{p}^*) = \mathfrak{p} \in U_\alpha \cap U_\beta$;

2) $\rho_1 \zeta^\alpha_h(\mathfrak{p}^*) = \rho_2 \sum_{g=1}^{r-d} N^\beta{}_g{}^\alpha{}_h(\mathfrak{p}) \zeta^\beta_g(\eta_{\beta\alpha}(\mathfrak{p}^*))$, $1 \leqq h \leqq r-d$.

$\eta_{\beta\alpha}$ is a bi-regular mapping since $\det N^{\beta\alpha}$ is a unit in the local ring of X at every point $\mathfrak{p}$ on $U_\alpha \cap U_\beta \cap V$, as follows from our assumptions that $x^\alpha_1, \cdots, x^\alpha_{r-d}$ (resp. $x^\beta_1, \cdots, x^\beta_{r-d}$) generate the ideal determined by V in the local ring of X at every point on U_α (resp. U_β), and that V is a non-singular variety ($\det N^{\beta\alpha}$ is the determinant of the square matrix $N^{\beta\alpha}$ of degree $r-d$ whose entry in the g-th row and h-th column is $N^\beta{}_g{}^\alpha{}_h$.) Now from the equations

$$x^\alpha_h = \sum_{g=1}^{r-d} N^\beta{}_g{}^\alpha{}_h x^\beta_g, \qquad 1 \leqq h \leqq r-d,$$

$$x^\alpha_{h_1}\zeta^\alpha_{h_2} - x^\alpha_{h_2}\zeta^\alpha_{h_1} = 0, \qquad 1 \leqq h_1, h_2 \leqq r-d,$$

$$x^\beta_{h_1}\zeta^\beta_{h_2} - x^\beta_{h_2}\zeta^\beta_{h_1} = 0, \qquad 1 \leqq h_1, h_2 \leqq r-d,$$

it is easy to check the following assertions. The composite mapping $\eta_{\alpha\beta}\eta_{\beta\alpha}$ is the identity map of $\Phi_\alpha^{-1}(U_\alpha \cap U_\beta)$; $\eta_{\alpha\gamma}\eta_{\gamma\beta}\eta_{\beta\alpha}$ is the identity map of $\Phi_\alpha^{-1}(U_\alpha \cap U_\beta \cap U_\gamma)$; the restriction of Φ_α to $\Phi_\alpha^{-1}(U_\alpha \cap U_\beta)$ and $\Phi_\beta\eta_{\beta\alpha}$ are equal regular mappings from $\Phi_\alpha^{-1}(U_\alpha \cap U_\beta)$ onto $U_\alpha \cap U_\beta$.

Let U_0 denote the complement $X - V$ in X, and let Φ_0 denote the identity map of U_0. For each $\alpha \in J^*$, let $\eta_{0\alpha}$ denote the bi-regular mapping of $\Phi_\alpha^{-1}(U_0 \cap U_\alpha)$ onto $\Phi_0^{-1}(U_0 \cap U_\alpha) = U_0 \cap U_\alpha$ which is the restriction of Φ_α to $\Phi_\alpha^{-1}(U_0 \cap U_\alpha)$. U_0 and the U^*_α, for all $\alpha \in J^*$, can be merged into a single variety X^*. For let us identify the open set $\Phi_\alpha^{-1}(U_\alpha \cap U_\beta)$ on U^*_α with the open set $\Phi_\beta^{-1}(U_\alpha \cap U_\beta)$ on U^*_β for each $\alpha, \beta \in J^*$ according to the mapping $\eta_{\beta\alpha}$ and identify $\Phi_\alpha^{-1}(U_0 \cap U_\alpha)$ with $U_0 \cap U_\alpha$ according to $\eta_{0\alpha}$. The family $\{U^*_\alpha\}_{\alpha \in J^*}$ together with U_0 forms an open covering on X^*. X^* is a non-singular algebraic variety of dimension r and there is a unique regular mapping Φ from X^* onto X whose restriction to each U^*_α is Φ_α (the restriction of Φ to U_0 is Φ_0).

We have the non-singular subvariety V^* of dimension $r-1$ on X^* such that $U^*_\alpha \cap V^* = V^*_\alpha$ for each $\alpha \in J^*$, and $U_0 \cap V^*$ is empty. The restriction of Φ to V^* equips that variety with the structure of a projective fiber bundle whose base space is V and whose fiber is a projective space of dimension $r-d-1$. Let $\mathfrak{p}^* \in U^*_\alpha \cap U^*_\beta \cap V^*$. Then we have

$$\rho_1 \zeta^\alpha_h(\mathfrak{p}^*) = \rho_2 \sum_{g=1}^{r-d} N^\beta{}_g{}^\alpha{}_h(\mathfrak{p}^*) \zeta^\beta{}_g(\mathfrak{p}^*), \qquad 1 \leqq h \leqq r-d.$$

This permits us to identify V^* with the dual projective bundle $\mathfrak{B}(N(X;Y))$ of the sheaf $N(X;V)$ according to the rule that $\zeta^\alpha{}_1, \cdots, \zeta^\alpha{}_{r-d}$ are the homogeneous coordinates which are paired to the previous sections $z^\alpha{}_1, \cdots, z^\alpha{}_{r-d}$ with reference to the construction of $\mathfrak{B}(N(X;V))$. The restriction of Φ to V^* is then identical to the bundle projection of $\mathfrak{B}(N(X;V))$.

The mapping Φ is called an anti-monoidal transformation, and the variety V^* is called the anti-center of Φ. Φ is bi-regular if $d = r-1$.

§ 11. Let $\vartheta(V^*)$ be the divisor class on X^* of the divisor V^*. We recall the construction of the sheaf $\mathcal{O}(-\vartheta(V^*))$. The restriction of $\mathcal{O}(-\vartheta(V^*))$ to any $U^*_{\alpha,h}$ is a free sheaf of dimension one generated by a section $D[\alpha,h]$; its restriction to U_0 is generated by $D[0]$; on $U^*_{\alpha,h_0} \cap U^*_{\beta,h_1}$, we have the transition law

$$D[\alpha, h_0] = \left(\sum_{h=1}^{r-d} N^\beta{}_h{}^\alpha{}_{h_0} \zeta^\beta{}_h / {}^\beta{}_{h_1}\right) D[\beta, h_1],$$

and on $U_0 \cap U^*_{\alpha,h_0}$, we have

$$D[\alpha, h_0] = x^\alpha{}_{h_0} D[0].$$

Now we have

$$x^{\alpha}{}_{h_0} = \left(\sum_{h=1}^{r-d} N^{\beta}{}_{h}{}^{\alpha}{}_{h_0} \zeta^{\beta}{}_{h} / \zeta^{\beta}{}_{h_1}\right) x^{\beta}{}_{h_1}$$

so that $\mathcal{O}(-\vartheta(V^*))$ is isomorphic to sheaf $\mathcal{L}(V^*)$ of germs of rational functions on X^* which are multiples of the divisor V^*. We have that

$$\Theta(\mathcal{L}(V^*)) = -\vartheta(V^*).$$

We obtain by inspection that the induced sheaf of $\mathcal{O}(-\vartheta(V^*))$ on the subvariety V^* is the basic sheaf $B(N(X;V))$ of $N(X;V)$; consequently, the basic divisor class $\Theta(N(X;V))$ is equal to the trace of $-\vartheta(V^*)$ on V^* (i.e., the reciprocal image of the divisor class $-\vartheta(V^*)$ with respect to the identity map of V^* in X^*).

Let Δ_X denote the diagonal on the product variety $X \times X$. Δ_X is non-singular and it is in bi-regular correspondence with X in a specific way. The sheaf $N(X \times X; \Delta_X)$ is therefore intrinsically associated with the variety X; in fact, the reciprocal image of $N(X \times X; \Delta_X)$ with respect to the canonical mapping of X onto Δ_X is none other than the sheaf $\Omega^1{}_X$ of germs of differentials of degree one on X.

§ 12. The sheaf $\Phi\Omega^1{}_X$, which is the reciprocal image of $\Omega^1{}_X$ with respect to the mapping Φ of X^* into X, admits an isomorphism into the sheaf $\Omega^1{}_{X^*}$ of germs of differentials of degree one on X^* in a specific way. In fact, we shall establish the exact sequence of sheaves

$$0 \to \Phi\Omega^1{}_X \to \Omega^1{}_{X^*} \to \delta N \otimes B^{-1}(N) \to 0;$$

δN denotes the derived sheaf of $N(X;V)$ and $B^{-1}(N)$ denotes the reciprocal sheaf of the basic sheaf $B(N(X;V))$; both of these last sheaves are defined on V^* since we can identify V^* and $\mathcal{B}(N(X;V))$; their tensor product extended to a sheaf on X^* is the third term in the above exact sequence.

We can suppose that our covering of X has the property that for each $\alpha \in J^*$, there exist d regular functions $y^{\alpha}{}_1, \cdots, y^{\alpha}{}_d$ on U_α such that the r functions

$$x^{\alpha}{}_h - x^{\alpha}{}_h(\mathfrak{p}), \qquad 1 \leqq h \leqq r-d,$$

$$y^{\alpha}{}_i - y^{\alpha}{}_i(\mathfrak{p}), \qquad 1 \leqq i \leqq d,$$

generate the maximal prime ideal in the local ring $\mathcal{O}_{\mathfrak{p}}$ for every point $\mathfrak{p}$ on U_α; we can always refine the covering so as to secure this possibility. On the open set $U^*{}_{\alpha,h_0}$, we have that the r functions

$$y^{\alpha}_{i} - y^{\alpha}_{i}(\mathfrak{p}^*), \qquad 1 \leqq i \leqq d,$$
$$x^{\alpha}_{h_0} - x^{\alpha}_{h_0}(\mathfrak{p}^*),$$
$$\zeta^{\alpha}_{h}/\zeta^{\alpha}_{h} - \zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0}(\mathfrak{p}^*), \qquad 1 \leqq h \leqq r-d, h \neq h_0,$$

generate the maximal prime ideal of the local ring $\mathcal{O}_{\mathfrak{p}^*}$ of X^* at every point $\mathfrak{p}^*$ on U^*_{α,h_0}. (We use the same symbol for a rational function on X and its reciprocal image on X^*.) The restriction of $\Omega^1{}_{X^*}$ to U^*_{α,h_0} is the free sheaf of dimension r generated by the differentials

$$dy^{\alpha}_{i}, \qquad 1 \leqq i \leqq d,$$
$$dx^{\alpha}_{h_0},$$
$$d(\zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0}), \qquad 1 \leqq h \leqq r-d, h \neq h_0.$$

The restriction of $\Phi\Omega^1{}_X$ to $U^*_{\alpha,h}$ is a free sheaf which is the subsheaf of the restriction of $\Omega^1{}_{X^*}$ to U^*_{α,h_0} generated by

$$dy^{\alpha}_{i}, \qquad 1 \leqq i \leqq d,$$
$$dx^{\alpha}_{h}, \qquad 1 \leqq h \leqq r-d.$$

But we have on X^* that

$$x^{\alpha}_{h} = x^{\alpha}_{h_0}\zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0}, \qquad 1 \leqq h \leqq r-d,$$

which gives

$$dx^{\alpha}_{h} = \zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0}dx^{\alpha}_{h_0} + x^{\alpha}_{h_0}d(\zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0}), \qquad 1 \leqq h \leqq r-d, h \neq h_0;$$

consequently, the restriction of $\Phi\Omega^1{}_X$ to U^*_{α,h_0} is generated by the sections

$$dy^{\alpha}_{i}, \qquad 1 \leqq i \leqq d,$$
$$dx^{\alpha}_{h_0},$$
$$x^{\alpha}_{h_0}d(\zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0}) = dx^{\alpha}_{h} - (\zeta^{\alpha}_{h}/\zeta^{\alpha}_{h_0})\,dx^{\alpha}_{h_0}, \qquad 1 \leqq h \leqq r-d, h \neq h_0.$$

The restrictions of $\Phi\Omega^1{}_X$ and $\Omega^1{}_{X^*}$ to $X^* - V^*$ are equal since Φ bi-regularly maps $X^* - V^*$ onto $X - V$.

It is now evident that the quotient sheaf of $\Omega^1{}_{X^*}$ modulo $\Phi\Omega^1{}_X$ is the extension to X^* of a locally free sheaf of dimension $r-d-1$ defined on V^*. By inspection, we obtain that this quotient sheaf is the extension to X^* of the locally free sheaf $\delta N \otimes B^{-1}(N)$ defined on V^*; thus we have our exact sequence

$$0 \to \Phi\Omega^1{}_X \to \Omega^1{}_{X^*} \to \delta N \otimes B^{-1}(N) \to 0.$$

Consider the sheaf $(\Phi\Omega^1{}_X)'$ which is the induced sheaf of $\Phi\Omega^1{}_X$ on the

subvariety V^*; $(\Phi\Omega^1{}_X)'$ is identical with the reciprocal image of the induced sheaf of $\Omega^1{}_X$ on V with respect to the restriction of Φ to V^*, which mapping can be identified with the bundle projection π_N of $N(X;V)$. We have a specific isomorphism of $\pi_N N(X;V)$ into $(\Phi\Omega^1{}_X)'$ according to the rule that

$$\pi_N{}^{-1}z^\alpha{}_h \to (dx^\alpha{}_h)', \qquad 1 \leqq h \leqq r-d,$$

on each $U^*{}_\alpha \cap V^*$; the $\pi_N{}^{-1}z^\alpha{}_h$ are the reciprocal images of the previous sections $z^\alpha{}_h$ for N over U_α. Thus we have the exact sequence

$$0 \to \pi_N N(X;V) \to (\Phi\Omega^1{}_X)' \to \pi_N\Omega^1{}_V \to 0$$

of locally free sheaves defined on V^*. We view $\pi_N N(X;V)$ as subsheaf of $(\Phi\Omega^1{}_X)'$ so that δN is the subsheaf $(\Phi\Omega^1{}_X)'$ whose restriction to $U^*{}_{\alpha,h_0}$ is the free sheaf generated by the sections

$$(dx^\alpha{}_h)' - (\zeta^\alpha{}_h/\zeta^\alpha{}_{h_0})(dx^\alpha{}_{h_0})', \qquad 1 \leqq h \leqq r-d, h \neq h_0.$$

Let $(\Omega^1{}_{X^*})'$ be the induced sheaf of $\Omega^1{}_{X^*}$ on V^*. Then the induced homomorphism from $(\Phi\Omega^1{}_X)'$ to $(\Omega^1{}_{X^*})'$ is described on $U^*{}_{\alpha,h_0} \cap V^*$ according to

$$\begin{aligned} &(dy^\alpha{}_i)' \to (dy^\alpha{}_i)', && 1 \leqq i \leqq d, \\ &(dx^\alpha{}_{h_0})' \to (dx^\alpha{}_{h_0})', && \\ &(dx^\alpha{}_h)' - (\zeta^\alpha{}_h/\zeta^\alpha{}_{h_0})(dx^\alpha{}_{h_0})' \to 0, && 1 \leqq h \leqq r-d, h \neq h_0. \end{aligned}$$

The kernel of the induced hmomorphism is δN and the image is a locally free sheaf R of dimension $d+1$ defined on V^*; we have the following exact sequences of locally free sheaves defined on V^*

$$0 \to \delta N \to (\Phi\Omega^1{}_X)' \to R \to 0,$$
$$0 \to R \to (\Omega^1{}_{X^*})' \to \delta N \otimes B^{-1}(N) \to 0.$$

The induced homomorphism from $(\Phi\Omega^1{}_X)'$ to $(\Omega^1{}_{X^*})'$ maps $\pi_N N(X;V)$ onto a locally free sheaf defined on V^* which is isomorphic to $B(N)$. Thus we can view $B(N)$ as a subsheaf of R and we have the exact sequence

$$0 \to B(N) \to R \to \pi_N\Omega^1{}_V \to 0.$$

II. Locally Free Resolutions of Sheaves.

§ 13. Let X and V be as in § 9-§ 12. Let Q be a locally free sheaf defined on V, and consider the extension of Q to a sheaf defined on X whose stalks are the zero module over each point of X not on V (which sheaf we

continue to denote as Q). Given any (coherent, algebraic) sheaf S defined on X, then, according to one of Serre's fundamental theorems, it is possible to choose a locally free sheaf F and a homomorphism ψ of F onto S. This permits us to construct an exact sequence

$$F^t \xrightarrow{\psi^t} \cdots \to F^s \xrightarrow{\psi^s} F^{s-1} \to \cdots \to F^0 \xrightarrow{\psi^0} Q \to 0,$$

where F^s is a locally free sheaf defined on X for $0 \leqq s \leqq t$. If $s \geqq r-d-1$ (dim. $V=d$), then the sheaf $\mathrm{Ker}[\psi^s]$ (i.e., the kernel of ψ^s) is a locally free sheaf defined on X; and if $s \geqq r-d$, then the stalk $F^s{}_{\mathfrak{p}}$ at every point $\mathfrak{p}$ on X is the direct sum of the stalk $\mathrm{Ker}[\psi^s]_{\mathfrak{p}}$ and a free $\mathcal{O}_{\mathfrak{p}}$-module. These assertions follow from the assumption that X and V are non-singular in conjunction with well known arguments from cohomological algebra; they will be proved here in the course of establishing further results of this type.

We shall deal with a fixed exact sequence

$$(1) \qquad F^{r-d} \xrightarrow{\psi^{r-d}} \cdots \to F^s \xrightarrow{\psi^s} F^{s-1} \to \cdots \to F^0 \xrightarrow{\psi^0} Q \to 0$$

of length $r-d$, where F^s is a locally free sheaf defined on X for $0 \leqq s \leqq r-d$. We pass to the sheaves ΦQ, ΦF^s, $0 \leqq s \leqq r-d$, which are the reciprocal images of the sheaves Q, F^s, $0 \leqq s \leqq r-d$, with respect to the anti-monoidal transformation Φ from X^* onto X with anti-center V^*. We also have the reciprocal image homomorphisms

$$\Phi F^0 \xrightarrow{\Phi^{-1}(\psi^0)} \Phi Q,$$

$$\Phi F^s \xrightarrow{\Phi^{-1}(\psi^s)} \Phi F^{s-1}, \qquad 1 \leqq s \leqq r-d.$$

For notational convenience, set

$$Q_* = \Phi Q,$$
$$F^s{}_* = \Phi F^s,$$
$$\psi^s{}_* = \Phi^{-1}(\psi^s).$$

Thus we have arrived at the diagram of sheaves and homomorphisms on X^*

$$(2) \qquad F^{r-d}{}_* \xrightarrow{\psi^{r-d}{}_*} \cdots \to F^s{}_* \xrightarrow{\psi^s{}_*} F^{s-1}{}_* \to \cdots \to F^0{}_* \xrightarrow{\psi^0{}_*} Q_* \to 0;$$

but (2) *is not an exact sequence if* $r-d>1$.

In the present chapter, we shall prove the following assertions.

1. The sheaf $\mathrm{Ker}[\psi^s{}_*]$ is a locally free sheaf defined on X^* for all $0 \leqq s \leqq r-d$; $\mathrm{Ker}[\psi^{r-d}]$ is a locally free sheaf defined on X and its reciprocal image with respect to Φ is $\mathrm{Ker}[\psi^{r-d}{}_*]$.

2. $\mathrm{Im}[\psi^s{}_*]$ is a locally free sheaf defined on X^* for $1 \leqq s \leqq r-d$; $\mathrm{Im}[\psi^1{}_*] = \mathrm{Ker}[\psi^0{}_*]$; $\mathrm{Im}[\psi^0{}_*] = Q_*$.

3. Let $Q^s{}_*$ denote the quotient sheaf of $\mathrm{Ker}[\psi^s{}_*]$ modulo $\mathrm{Im}[\psi^{s+1}{}_*]$ for $1 \leqq s \leqq r-d-1$; then $Q^s{}_*$ is isomorphic to $Q_* \otimes \wedge^s(\delta N)$, the tensor product of Q_* with the s-fold exterior product of the derived sheaf δN of $N(X;V)$; thus we hace the exact sequence

$$0 \to \mathrm{Im}[\psi^{s+1}{}_*] \to \mathrm{Ker}[\psi^s{}_*] \to Q_* \otimes \wedge^s(\delta N) \to 0$$

for $1 \leqq s \leqq r-d-1$.

There is another diagram of interest. Let Q', F'^s, $0 \leqq s \leqq r-d$, denote the induced sheaf of Q_*, $F^s{}_*$, $0 \leqq s \leqq r-d$, on the subvariety V^*; let ψ'^s denote the induced homomorphism of $\psi^s{}_*$ for $0 \leqq s \leqq r-d$. Then we have $Q' = Q_*$ and the diagram

$$(3) \qquad F'^{r-d} \xrightarrow{\psi'^{r-d}} \cdots \to F'^s \xrightarrow{\psi'^s} F'^{s-1} \to \cdots \to F'^0 \xrightarrow{\psi'^0} Q_* \to 0,$$

where Q_*, F'^s, $0 \leqq s \leqq r-d$ are locally free sheaves defined on V^*. The diagram (3) *is not exact*. The following assertions are true.

1′. $\mathrm{Ker}[\psi'^s]$ is a locally free sheaf defined on V^* for all $0 \leqq s \leqq r-d$.

2′. $\mathrm{Im}[\psi'^s]$ is a locally free sheaf defined on V^* for all $0 \leqq s \leqq r-d$; $\mathrm{Im}[\psi'^0] = Q_*$; $\mathrm{Im}[\psi'^1] = \mathrm{Ker}[\psi'^0]$.

3′. The quotient sheaf of $\mathrm{Ker}[\psi'^s]$ modulo the subsheaf $\mathrm{Im}[\psi'^{s+1}]$ is for $1 \leqq s \leqq r-d$ isomorphic to the sheaf $Q_* \otimes \wedge^s(N^*)$, the tensor product of Q_* with the s-fold exterior product of the sheaf $N^* = \pi_N N(X;V)$ which is the reciprocal image of $N(X;V)$ with respect to π_N; thus we have the exact sequence of locally free sheaves on V^*

$$0 \to \mathrm{Im}[\psi'^{s+1}] \to \mathrm{Ker}[\psi'^s] \to Q_* \otimes \wedge^s(N^*) \to 0 \qquad \text{for } 1 \leqq s \leqq r-d.$$

§ 14. The present § consists of formal algebra, and its aim is the proof of Lemma 1 which is the key to the proofs of the assertions of § 13.

Let $\boldsymbol{O}$ be a commutative ring with a multiplicative neutral element $1 \neq 0$ (eventually, $\boldsymbol{O}$ will be a local ring). We shall consider unitary $\boldsymbol{O}$-modules exclusively (i.e., 1 acts as the identity operator in any $\boldsymbol{O}$-module considered

here). Let $z_1,\cdots,z_t$ be elements in $\boldsymbol{O}$ which satisfy the Cartan-Eilenberg condition:

(C. E.) if for any $u \in \boldsymbol{O}$, we have that uz_i belongs to the ideal $(z_1,\cdots,z_{i-1})$ in $\boldsymbol{O}$ generated by $z_1,\cdots,z_{i-1}$, then u belongs to the ideal $(z_1,\cdots,z_{i-1})$ (in particular, for $i=1$, we require that z_1 is not a divisor of zero). We shall assume that the ideal $(z_1,\cdots,z_t)$ is not the unit ideal. Let $\boldsymbol{R}$ be the residue class ring of $\boldsymbol{O}$ modulo the ideal $(z_1,\cdots,z_t)$; then $\boldsymbol{R}$ has a multiplicative neutral element not zero; $\boldsymbol{R}$ carries the structure of an $\boldsymbol{O}$-module in a specific way and the residue class mapping μ_0 is an $\boldsymbol{O}$-homomorphism of $\boldsymbol{O}$ onto $\boldsymbol{R}$.

For $1 \leqq s \leqq t$, let M_s be the free $\boldsymbol{O}$-module of dimension $t!/s!(t-s)!$ generated by the symbols

$$[h_1,\cdots,h_s],$$

one such symbol for each strictly increasing sequence $1 \leqq h_1 < \cdots < h_s \leqq t$ of s integers chosen from the set $\{1,\cdots,t\}$. We construct an $\boldsymbol{O}$-homomorphism μ_s from M_s to M_{s-1} $(s>1)$ according to the rule

$$\mu_s : [h_1,\cdots,h_s] \rightarrow \sum_{p=1}^{s} (-1)^{p-1} z_{h_p} [h_1,\cdots,\hat{h}_p,\cdots,h_s],$$

where $[h_1,\cdots,\hat{h}_p,\cdots,h_s]$ is that generator of M_{s-1} obtained by suppressing the p-th member h_p of the sequence $1 \leqq h_1 < \cdots < h_s \leqq t$. For $s=1$, we construct the homomorphism from M_1 to $\boldsymbol{O}$ according to

$$\mu_1 : [h] \rightarrow z_h, \qquad 1 \leqq h \leqq t.$$

It is a consequence of the Cartan-Eilenberg condition on $z_1,\cdots,z_t$ that

$$(1) \qquad 0 \rightarrow M_t \xrightarrow{\mu_t} \cdots \rightarrow M_s \xrightarrow{\mu_s} M_{s-1} \rightarrow \cdots \rightarrow M_1 \xrightarrow{\mu_1} \boldsymbol{O} \xrightarrow{\mu_0} \boldsymbol{R} \rightarrow 0$$

is an exact sequence of $\boldsymbol{O}$-modules; the proof is given in their book. The exact sequence (1) is called the Koszul resolution of $\boldsymbol{R}$ by free $\boldsymbol{O}$-modules.

Let L be a free $\boldsymbol{R}$-module of dimension q with the free basis $l_1,\cdots,l_q$. Then by the Koszul resolution of L with respect to the basis $l_1,\cdots,l_q$, we mean the direct sum of the Koszul resolution of $\boldsymbol{O}$ taken q times. Explicitly, M_s^q $(1 \leqq s \leqq t)$ is a free $\boldsymbol{O}$-module of dimension $qt!/s!(t-s)!$ generated by the symbols

$$[h_1,\cdots,h_s;i];$$

one such symbol for each pair consisting of a strictly increasing sequence

$1 \leqq h_1 < \cdots < h_s \leqq t$ and an integer i, $1 \leqq i \leqq q$. The module $M^q{}_0$ is the free $\boldsymbol{O}$-module of dimension q generated by the symbols

$$[\,;i], \qquad\qquad 1 \leqq i \leqq q.$$

We construct an $\boldsymbol{O}$-homomorphism λ_s from $M^q{}_s$ to $M^q{}_{s-1}$ $(s > 1)$ according to

$$\lambda_s : [h_1, \cdots, h_s ; i] \to \sum_{p=1}^{s} (-1)^{p-1} z_{h_p} [h_1, \cdots, \hat{h}_p, \cdots, h_s ; i] ;$$

we define $\lambda_1 : M^q{}_1 \to M^q{}_0$ according to

$$\lambda_1 : [h ; i] \to z_h [\,; i],$$

and $\lambda_0 : M^q{}_0 \to L$ according to

$$\lambda_0 : [\,; i] \to l_i.$$

The exact sequence

$$(2) \qquad 0 \to M^q{}_t \xrightarrow{\lambda_t} \cdots \to M^q{}_1 \xrightarrow{\lambda_1} M^q{}_0 \xrightarrow{\lambda_0} L \to 0$$

is the Koszul resolution of L with respect to the basis $l_1, \cdots, l_q$.

We now assume that $\boldsymbol{O}$ is a local ring; recall that $z_1, \cdots, z_t$ are assumed to be non-units of $\boldsymbol{O}$. Consider an arbitrary resolution of L of length t. By this, we mean any exact sequence

$$(3) \qquad E_t \xrightarrow{\phi_t} \cdots \to E_s \xrightarrow{\phi_s} E_{s-1} \to \cdots \to E_0 \xrightarrow{\phi_0} L \to 0,$$

where $E_0, \cdots, E_t$ are free $\boldsymbol{O}$-modules (all our modules are finitely generated). The following lemma gives the crucial property of the Koszul resolution; in particular, it gives that $\operatorname{Ker}[\phi_t]$ and $\operatorname{Ker}[\phi_{t-1}]$ are free $\boldsymbol{O}$-modules; more generally, the lemma gives that $\operatorname{Ker}[\phi_s]$ is isomorphic to the direct sum of $\operatorname{Ker}[\lambda_s]$ and a free $\boldsymbol{O}$-module for all $0 \leqq s \leqq t$.

LEMMA 1. *$\boldsymbol{O}$ is a (commutative) local ring with a multiplicative neutral element $1 \neq 0$; $z_1, \cdots, z_t$ is a set of non-units of $\boldsymbol{O}$ which satisfy the condition (C.E.); $\boldsymbol{R}$ is the residue class ring of $\boldsymbol{O}$ modulo the ideal $(z_1, \cdots, z_t)$; L is a free $\boldsymbol{R}$-module of dimension q; finally*

$$(2) \qquad 0 \to M^q{}_t \xrightarrow{\lambda_t} \cdots \to M^q{}_s \xrightarrow{\lambda_s} M^q{}_{s-1} \to \cdots \to M^q{}_0 \xrightarrow{\lambda_0} L \to 0$$

is the Koszul resolution of L with respect to some free basis of the $\boldsymbol{R}$-module L (viewed as $\boldsymbol{O}$-module). Then given any exact sequence

$$(3) \qquad E_t \xrightarrow{\phi_t} \cdots \to E_s \xrightarrow{\phi_s} E_{s-1} \to \cdots \to E_0 \xrightarrow{\phi_0} L \to 0,$$

where $E_0, \cdots, E_t$ *are free* $\boldsymbol{O}$*-modules, it is possible to construct homomorphisms*

$$\eta_s\colon M^q{}_s \to E_s, \qquad \xi_s\colon E_s \to M^q{}_s$$

for $0 \leqq s \leqq t$ *which satisfy:*

1.) $\xi_s\eta_s$ *is the identity map on* $M^q{}_s$;

2.) $\xi_{s-1}\phi_s = \lambda_s\xi_s$, $\eta_{s-1}\lambda_s = \phi_s\eta_s$ (*we shall agree that* ξ_{-1} *and* η_{-1} *denote the identity map of* L).

SUPPLEMENT TO LEMMA 1. *The module* $\mathrm{Ker}[\xi_s]$ *is a free* $\boldsymbol{O}$*-module;* $\mathrm{Ker}[\phi_s]$ *is the direct sum of* $\mathrm{Ker}[\xi_s]$ *and the image of* $\mathrm{Ker}[\lambda_s]$ *by* η_s, *which image is isomorphic to* $\mathrm{Ker}[\lambda_s]$.

The homomorphisms ξ_s and η_s are constructed by induction on s. It is convenient to cast part of the proof in the guise of several elementary lemmas; only one of these requires a demonstration.

LEMMA 2. *E, G are free modules of dimensions n and m over the local ring* $\boldsymbol{O}$; ψ *is a homomorphism from G onto E. Then given a free basis* $e_1, \cdots, e_n$ *for E, it is possible to choose a free basis* $g_1, \cdots, g_m$ *for G such that*

$$\psi(g_i) = e_i, \qquad 1 \leqq i \leqq n,$$

$$\psi(g_{n+u}) = 0, \qquad 1 \leqq n \leqq m - n;$$

or, without reference to bases, $\mathrm{Ker}[\psi]$ *is a free* $\boldsymbol{O}$*-module and there exists an isomorphism* ψ' *from E into G such that* $\psi\psi'$ *is the identity map of E; consequently, G is the direct sum of* $\mathrm{Ker}[\psi]$ *and* $\mathrm{Im}[\psi']$.

LEMMA 3. *E is a free module of dimension n over the local ring* $\boldsymbol{O}$ *and* $e_1, \cdots, e_n$ *is a free basis for E. Let* $e'_1, \cdots, e'_n$ *be elements of E such that for each i,* $1 \leqq i \leqq n$,

$$e'_i - e_i$$

is equal to a linear combination of $e_1, \cdots, e_n$ *whose coefficients are non-units of the local ring* $\boldsymbol{O}$. *Then* $e'_1, \cdots, e'_n$ *is a free basis for E.*

LEMMA 4. (This lemma reiterates the well known fact that a free module is a projective module, and it does not require the assumption that $\boldsymbol{O}$ be a local ring.) *E is a free* $\boldsymbol{O}$*-module; A, A' are* $\boldsymbol{O}$*-modules;* θ *is a homomirphism of A onto A';* π' *is a homomorphism of E into A'. Then there exists a homomorphism* π *of E into A such that* $\theta\pi$ *is equal to* π'.

LEMMA 5. (Retain the hypotheses and notations of Lemma 1.) *Let* π' *be a homomorphism of* E_s *onto the submodule* $\mathrm{Im}[\lambda_s]$ *of* $M^q{}_{s-1}$; *if* $s=0$, *then* $\mathrm{Im}[\lambda_0]=L$. *We can apply Lemma 4 since* E_s *is a free* $\boldsymbol{O}$*-module and* λ_s *maps* $M^q{}_s$ *onto* $\mathrm{Im}[\lambda_s]$, *which assures the existence of a homomorphism* π *of* E_s *into* $M^q{}_s$ *with the property* $\lambda_s\pi=\pi'$. *Then we claim that* π *maps* E_s *onto* $M^q{}_s$.

Proof. We have that $\mathrm{Im}[\lambda_s]$ is the submodule of $M^q{}_{s-1}$ generated by the elements

$$\sum_{p=1}^{s}(-1)^{p-1}z_{h_p}[h_1,\cdots,\hat{h}_p,\cdots,h_s],$$

one such element for each strictly increasing sequence $1\leqq h_1<\cdots<h_s\leqq t$ of length s and integer i, $1\leqq 0\leqq q$; (for $s=0$, we have $\mathrm{Im}[\lambda_0]=L$ is generated by $l_1,\cdots,l_q$). Since π' maps E_s onto $\mathrm{Im}[\lambda_s]$, we can choose elements

$$e'[h_1,\cdots,h_s\,;i],\qquad\qquad 1\leqq h_1<\cdots<h_s\leqq t, 1\leqq i\leqq q,$$

such that

$$\pi'(e'[h_1,\cdots,h_s\,;i])=\sum_{p=1}^{s}(-1)^{p-1}z_{h_p}[h_1,\cdots,\hat{h}_p,\cdots,h_s\,;i]\,;$$

(for $s=0$, we choose $e'[i]$, $i\leqq 1\leqq q$, such that

$$\pi'(e'[i])=l_i).$$

We choose a homomorphism π of E_s into $M^q{}_s$ with the property $\lambda_s\pi=\pi'$. The elements

$$\pi(e'[h_1,\cdots,h_s\,;i])-[h_1,\cdots,h_s\,;i]$$

are all in the submodule $\mathrm{Ker}[\lambda_s]$ since

$$\lambda_s([h_1,\cdots,h_s\,;i])=\sum_{p=1}^{s}(-1)^{p-1}z_{h_p}[h_1,\cdots,\hat{h}_p,\cdots,h_s\,;i].$$

But $\mathrm{Ker}[\lambda_s]$ is generated by the elements

$$\sum_{p=1}^{s}(-1)^{p-1}z_{h_p}[h_1,\cdots,\hat{h}_p,\cdots,h_{s+1}\,;i],$$

one such element for each strictly increasing sequence $1\leqq h_1<\cdots<h_{s+1}\leqq t$ of length $s+1$ and integer i, $1\leqq i\leqq q$. We can apply Lemma 3 since $z_1,\cdots,z_t$ are non-units of $\boldsymbol{O}$, and this proves that the elements

$$\pi(e'[h_1,\cdots,h_s\,;i]),\qquad\qquad 1\leqq h_1<\cdots<h_s\leqq t, 1\leqq i\leqq q,$$

generate $M^q{}_s$. Consequently, π maps E_s onto $M^q{}_s$.

Proof of Lemma 1. Assume that the homomorphisms $\xi_{-1}, \eta_{-1}, \cdots, \xi_{s-1}, \eta_{s-1}$ with the required properties have been constructed and $0 \leqq s \leqq t$; recall that ξ_{-1}, η_{-1} are both the identity map of L. We claim that the composite homomorphism $\xi_{s-1}\phi_s$ maps E_s onto $\mathrm{Im}[\lambda_s]$. This is obvious if $s=0$. If $s>0$, then for any element m of $\mathrm{Im}[\lambda_s]$, we have that $\eta_{s-1}(m)$ belongs to $\mathrm{Im}[\phi_s]$ since $\phi_{s-1}(\eta_{s-1}(m)) = \eta_{s-2}(\lambda_{s-1}(m)) = 0$ by our inductive assumption and the fact that $\mathrm{Im}[\phi_s] = \mathrm{Ker}[\phi_{s-1}]$, and $\mathrm{Im}[\lambda_s] = \mathrm{Ker}[\lambda_{s-1}]$; consequently, we can choose an element e in E_s such that $\phi_s(e) = \eta_{s-1}(m)$, which gives $\xi_{s-1}(\phi_s(e)) = m$; thus $\mathrm{Im}[\xi_{s-1}\phi_s]$ contains $\mathrm{Im}[\lambda_s]$. On the other hand, we have

$$\lambda_{s-1}\xi_{s-1}\phi_s = \xi_{s-2}\phi_{s-1}\phi_s = 0,$$

which proves that $\mathrm{Im}[\xi_{s-1}\phi_s]$ is contained in $\mathrm{Im}[\lambda_s]$. It follows from Lemma 4 (as applied in the statement of Lemma 5 with $\xi_{s-1}\phi_s = \pi'$) that we can choose a homomorphism ξ_s of E_s into $M^q{}_s$ with the property $\lambda_s\xi_s = \xi_{s-1}\phi_s$; and from Lemma 5, it follows that ξ_s maps E_s onto $M^q{}_s$. Since E_s, $M^q{}_s$ are free $\boldsymbol{O}$-modules and ξ_s maps E_s onto $M^q{}_s$, we apply Lemma 2 and obtain an isomorphism η_s of $M^q{}_s$ into E_s such that $\xi_s\eta_s$ is the identity map of $M^q{}_s$. It remains to check that $\phi_s\eta_s = \eta_{s-1}\lambda_s$. To this end, we observe that $\xi_{s-1}\phi_s\eta_s = \lambda_s\xi_s\eta_s = \lambda_s$ since $\xi_{s-1}\phi_s = \lambda_s\xi_s$ and $\xi_s\eta_s$ is the identity map of $M^q{}_s$; this leads to $\eta_{s-1}\xi_{s-1}\phi_s\eta_s = \eta_{s-1}\lambda_s$ and since the restriction of $\eta_{s-1}\xi_{s-1}$ to the submodule $\mathrm{Im}[\eta_{s-1}]$ is the identity map of that module, we get $\phi_s\eta_s = \eta_{s-1}\lambda_s$.

Applying Lemma 2 to the homomorphism ξ_s from E_s onto $M^q{}_s$, it follows that $\mathrm{Ker}[\xi_s]$ is a free $\boldsymbol{O}$-module. We have that ξ_s maps $\mathrm{Ker}[\phi_s]$ onto $\mathrm{Ker}[\lambda_s]$ (for we proved at the start of the proof of Lemma 1 that $\xi_{s-1}\phi_s$ maps E_s onto $\mathrm{Ker}[\lambda_{s-1}]$); thus we have that $\mathrm{Ker}[\phi_s]$ is the direct sum of $\mathrm{Ker}[\xi_s]$ and the image of $\mathrm{Ker}[\phi_s]$ by $\eta_s\xi_s$, which image is isomorphic to $\mathrm{Ker}[\lambda_s]$. This completes the proof of the supplement to Lemma 1.

§ 15. Consider the exact sequence of sheaves

$$(1) \qquad F^{r-d} \xrightarrow{\psi^{r-d}} \cdots \to F^0 \xrightarrow{\psi^0} Q \to 0$$

of § 13. At a point $\mathfrak{p}$ on X, we have the exact sequence of stalks

$$(2) \qquad F^{r-d}{}_{\mathfrak{p}} \xrightarrow{\psi^{r-d}{}_{\mathfrak{p}}} \cdots \to F^0{}_{\mathfrak{p}} \xrightarrow{\psi^0{}_{\mathfrak{p}}} Q_{\mathfrak{p}} \to 0.$$

If $\mathfrak{p}$ is not on V, then $Q_{\mathfrak{p}}$ is the zero module and $\mathrm{Ker}[\psi^s]_{\mathfrak{p}}$ is a free $\mathfrak{O}_{\mathfrak{p}}$-module for all $0 \leqq s \leqq r-d$, as follows from Lemma 2 since $\mathfrak{O}_{\mathfrak{p}}$ is a local ring.

Assume that $\mathfrak{p} \in V$. Then there exist $r-d$ regular functions $x_1, \cdots, x_{r-d}$ in $\mathcal{O}_\mathfrak{p}$ which generate the ideal determined by V in $\mathcal{O}_\mathfrak{p}$, and since $\mathfrak{p}$ is a simple point on V, they can be extended to a basis of r elements for the maximal prime ideal of $\mathcal{O}_\mathfrak{p}$; consequently, $x_1, \cdots, x_{r-d}$ satisfy the condition (C.E.) of § 14. The residue class ring of $\mathcal{O}_\mathfrak{p}$ modulo the ideal $(x_1, \cdots, x_{r-d})$ is the local ring $\mathcal{O}(V; \mathfrak{p})$ of V at $\mathfrak{p}$. The stalk $Q_\mathfrak{p}$ is free module of dimension q over $\mathcal{O}(V; \mathfrak{p})$. Thus the structure of the stalks $\mathrm{Ker}[\psi^s]_\mathfrak{p}$ is known on the basis of Lemma 1 of § 14 and its supplement. In particular, we have that $\mathrm{Ker}[\psi^{r-d}]$ is a locally free sheaf defined on X.

Taking account of the properties of locally free sheaves and the structure of the stalks $\mathrm{Ker}[\psi^s]_\mathfrak{p}$ as revealed by Lemma 1 of § 14, we can suppose that our covering $\{U_\alpha\}_{\alpha \in J}$ has the following properties:

1) The restriction of Q to any $U_\alpha \cap V$ (with $\alpha \in J^*$) is a free sheaf generated by sections $l^\alpha_1, \cdots, l^\alpha_q$;

2) The restrictions of F^s, $1 \leqq s \leqq r-d$, to U_α (again $\alpha \in J^*$) is a free sheaf of dimension n_s generated by sections

$$\begin{aligned} &f^\alpha[h_1, \cdots, h_s; i], && 1 \leqq h_1 < \cdots < h_s \leqq r-d, 1 \leqq i \leqq q, \\ &f^\alpha_{t_s+j}, && 1 \leqq j \leqq u_s - t_s, \\ &f^\alpha_{u_s+k}, && 1 \leqq k \leqq n_s - u_s, \end{aligned}$$

(the restriction of F^0 to U_α is generated by

$$\begin{aligned} &f^\alpha[\,;i], && 1 \leqq i \leqq q, \\ &f_{q+k}, && 1 \leqq k \leqq n_0 - q), \end{aligned}$$

where for $s \geqq 1$, we have

$$t_s = q(r-d)!/s!(r-d-s)!$$

$$u_s - t_s = n_{s-1} - u_{s-1},$$

and $u_0 = t_0 = q$;)

3) The restriction of ψ^0 to U_α is described by

$$\begin{aligned} &f^\alpha[\,;i] \rightarrow l^\alpha_i, && 1 \leqq i \leqq q, \\ &f^\alpha_{q+k} \rightarrow 0, && 1 \leqq k \leqq n_0 - q, \end{aligned}$$

and the restriction of $\mathrm{Ker}[\psi^0]$ to U_α is generated by the sections

$$\begin{aligned} &x^\alpha{}_h f^\alpha[\,;i], && 1 \leqq h \leqq r-d, 1 \leqq i \leqq q, \\ &f^\alpha_{q+k}, && 1 \leqq k \leqq n_0 - q. \end{aligned}$$

4) The restriction of ψ^s $(s \geqq 1)$ to U_α is described by

$$f^\alpha[h_1, \cdots, h_s\,; i] \to \sum_{p=1}^{s} (-1)^{p-1} x^\alpha{}_{h_p} f^\alpha[h_1, \cdots, \hat{h}_p, \cdots, h_s\,; i],$$

$$f^\alpha{}_{t_s+j} \to f^\alpha{}_{u_{s-1}+j}, \qquad 1 \leqq j \leqq u_s - t_s = n_{s-1} - u_{s-1},$$

$$f^\alpha{}_{u_s+k} \to 0, \qquad 1 \leqq k \leqq n_{s-1} - u_{s-1}\,;$$

consequently, the restriction of $\mathrm{Ker}[\psi^s]$ to U_α is generated by the

$$\sum_{p=1}^{s+1} (-1)^{p-1} x^\alpha{}_{h_p} f^\alpha[h_1, \cdots, \hat{h}_p, \cdots, h_s\,; i],$$

$$1 \leqq h_1 < \cdots < h_s \leqq r-d, 1 \leqq i \leqq q,$$

$$f^\alpha{}_{u_s+k}, \qquad 1 \leqq k \leqq n_s - u_s.$$

The functions $x^\alpha{}_1, \cdots, x^\alpha{}_{r-d}$ are as in § 9. We shall agree that $f^\alpha[h_1, \cdots, h_s\,; i]$ is defined for arbitrary sequences $h_1, \cdots, h_s$ chosen from $\{1, \cdots, r-d\}$ but that it is strictly skew-symmetric in the h's.

The restriction of $Q_* = \Phi Q$ to any $U^*{}_\alpha \cap V^*$ is a free sheaf generated by sections

$$l_*{}^\alpha{}_i, \qquad 1 \leqq i \leqq q,$$

where $l_*{}^\alpha{}_i$ is the reciprocal image of the section $l^\alpha{}_i$ of Q over U_α; similarly, the restriction of $F^s{}_*$ to $U^*{}_\alpha$ is the free sheaf generated by the sections

$$f^\alpha{}_*[h_1, \cdots, h_s\,; i], \qquad 1 \leqq h_1 < \cdots < h_s \leqq r-d, 1 \leqq i \leqq q,$$

$$f^\alpha{}_{*t_s+j}, \qquad 1 \leqq j \leqq u_s - t_s,$$

$$f^\alpha{}_{*u_s+k}, \qquad 1 \leqq k \leqq n_s - u_s.$$

It follows that the restriction of $F^s{}_*$ to $U^*{}_{\alpha,h_0}$ is the free sheaf generated by the sections

$$f^\alpha{}_*[h_0, h_1, \cdots, h_{s-1}\,; i], \qquad 1 \leqq h_1 < \cdots < h_{s-1} \leqq r-d, 1 \leqq i \leqq q,$$

where $h_p \neq h_0$ for $1 \leqq p \leqq s-1$, the sections

$$f^\alpha{}_*[h_1, \cdots, h_s\,; i] + \sum_{p=1}^{s} (-1)^p (\zeta^\alpha{}_{h_p}/\zeta^\alpha{}_{h_0}) f^\alpha{}_*[h_0, h_1, \cdots, \hat{h}_p, \cdots, h_s\,; i]$$

for all $1 \leqq h_1 < \cdots < h_s \leqq r-d$, $1 \leqq i \leqq q$, and $h_p \neq h_0$ for $1 \leqq p \leqq s$, and the sections

$$f^\alpha{}_{*t_s+j}, \qquad 1 \leqq j \leqq u_s - t_s,$$

$$f^\alpha{}_{*u_s+k}, \qquad 1 \leqq k \leqq n_s - u_s.$$

On $U^*{}_{\alpha,h_0}$, we have that

$$x^\alpha{}_h = (\zeta^\alpha{}_h/\zeta^\alpha{}_{h_0}) x^\alpha{}_{h_0} \qquad 1 \leqq h \leqq r-d, h \neq h_0\,;$$

consequently, the restriction of $\psi^s{}_*$ $(s \geqq 1)$ to $U^*{}_{\alpha,h_0}$ is described by

$$f^\alpha{}_*[h_0, h_1, \cdots, h_{s-1}\,; i] \to x^\alpha{}_{h_0}(f^\alpha{}_*[h_1, \cdots, h_{s-1}\,; i]$$
$$+\sum_{p=1}^{s-1} (-1)^p (\zeta^\alpha{}_{ph}/\zeta^\alpha{}_{h_0}) f^\alpha{}_*[h_0, \cdots, \hat{h}_p, \cdots, h_{s-1}\,; i])$$

for all $1 \leqq h_1 < \cdots < h_{s-1} \leqq r-d$, $h_p \neq h_0$, $1 \leqq i \leqq q$,

$$f^\alpha{}_*[h_1, \cdots, h_s\,; i] + \sum_{p=1}^{s} (-1)^p (\zeta^\alpha{}_{h_p}/\zeta^\alpha{}_{h_0}) f^\alpha{}_*[h_0, h_1, \cdots, \hat{h}_p, \cdots, h_s\,; i] \to 0$$

for all $1 \leqq h_1 < \cdots < h_s \leqq r-d$, $h_p \neq h_0$, $1 \leqq i \leqq q$,

$$f^\alpha{}_{*t_s+j} \to f^\alpha{}_{*u_{s-1}+j}, \qquad 1 \leqq j \leqq u_s - t_s = n_{s-1} - u_{s-1},$$
$$f^\alpha{}_{*u_s+k} \to 0, \qquad 1 \leqq k \leqq n_s - u_s.$$

This proves that the restriction of $\mathrm{Ker}[\psi^s{}_*]$, $s \geqq 1$, to $U^*{}_{\alpha,h_0}$ is a free sheaf generated by the sections

$$f^\alpha{}_*[h_1, \cdots, h_s\,; i] + \sum_{p=1}^{s} (-1)^p (\zeta^\alpha{}_{h_p}/\zeta^\alpha{}_{h_0}) f^\beta{}_*[h_0, h_1, \cdots, \hat{h}_p, \cdots, h_s\,; i]$$

for $1 \leqq h_1 < \cdots < h_s \leqq r-d$, $h_p \neq h_0$, $1 \leqq i \leqq q$,

$$f^\alpha{}_{*u_s+k}, \qquad 1 \leqq k \leqq n_s - u_s;$$

furthermore, the restriction of $\mathrm{Im}[\psi^{s+1}{}_*]$ to $U^*{}_{\alpha,h_0}$ is a free sheaf since it is the subsheaf of the restriction of $\mathrm{Ker}[\psi^s{}_*]$ to $U^*{}_{\alpha,h_0}$ generated by

$$x^\alpha{}_{h_0}(f^\alpha{}_*[h_1, \cdots, h_s\,; i]$$
$$+\sum_{p=1}^{s} (-1)^p (\zeta^\alpha{}_{h_p}/\zeta^\alpha{}_{h_0}) f^\alpha{}_*[h_0, h_1, \cdots, \hat{h}_p, \cdots, h_s\,; i])$$

for $1 \leqq h_1 < \cdots < h_s \leqq r-d$, $h_p \neq h_0$, $1 \leqq i \leqq q$,

$$f^\alpha{}_{*u_s+k}, \qquad 1 \leqq k \leqq n_s - u_s.$$

The restriction of $\mathrm{Ker}[\psi^0{}_*]$ to $U^*{}_{\alpha,h_0}$ is equal to the restriction of $\mathrm{Im}[\psi^1{}_*]$ to $U^*{}_{\alpha,h_0}$ which is the subsheaf of the restriction of $F^0{}_*$ to $U^*{}_{\alpha,h_0}$ generated by

$$x^\alpha{}_{h_0} f^\alpha{}_*[\,; i], \qquad 1 \leqq i \leqq q,$$
$$f^\alpha{}_{*q+k}, \qquad 1 \leqq k \leqq n_0 - q.$$

We conclude therefore that $\mathrm{Ker}[\psi^s{}_*]$, resp. $\mathrm{Im}[\psi^s{}_*]$, is a locally free sheaf defined on X^* for all $0 \leqq s \leqq r-d$, resp. $1 \leqq s \leqq r-d$; $\mathrm{Ker}[\psi^0{}_*] = \mathrm{Im}[\psi^1{}_*]$; $\mathrm{Ker}[\psi^{r-d}{}_*] = \Phi\,\mathrm{Ker}[\psi^{r-d}]$. The residue class sheaf $Q^s{}_*$ of $\mathrm{Ker}[\psi^s{}_*]$ modulo $\mathrm{Im}[\psi^{s+1}{}_*]$ for $1 \leqq s \leqq r-d-1$ is evidently the extension

to X^* of a locally free sheaf of dimension $q(r-d-1)!/s!(r-d-1-s)!$ defined on V^*. By a rather straightforward calculation, one constructs an isomorphism of $Q^s{}_*$ onto $Q_* \otimes \wedge^s(\delta N)$; thus we have the exact sequence

$$(3) \qquad 0 \to \mathrm{Im}[\psi^{s+1}{}_*] \to \mathrm{Ker}[\psi^s{}_*] \to Q_* \otimes \wedge^s(\delta N) \to 0$$

for $1 \leqq s \leqq r-d-1$. This completes our discussion of the assertions 1., 2., and 3. of § 13; the assertions 1′., 2′., 3′. follow rather easily from the calculations of this § but we shall have no need of them in the sequel.

III. The Dual Rational Transformation.

§ 16. The variety X and the sheaf E are as in § 3; G is a locally free sheaf of dimension m defined on X, and ψ is a homomorphism from G into E with the property that $\mathrm{Im}[\psi]$ is not the zero sheaf. We are going to construct a rational transformation $\mathcal{B}(\psi)$ from $\mathcal{B}(E)$ into $\mathcal{B}(G)$; it is called the dual rational transformation of the sheaf homomorphism $\psi\colon G \to E$.

It is permissible to asume that the previous covering $\{U_\alpha\}_{\alpha \in J}$ is such that the restriction of G to any U_α is a free sheaf of dimension m generated by sections $g^\alpha{}_1, \cdots, g^\alpha{}_m$ of G over U_α. With reference to G, we have the transition laws

$$g^\alpha{}_q = \sum_{p=1}^{m} G^\beta{}_p{}^\alpha{}_q g^\beta{}_p, \qquad 1 \leqq q \leqq m,$$

on $U_\alpha \cap U_\beta$; the functions $G^\beta{}_p{}^\alpha{}_q$, $1 \leqq p, q \leqq m$ are regular on $U_\alpha \cap U_\beta$. The restriction of ψ to any U_α is described by

$$\psi\colon g^\alpha{}_p \to \sum_{i=1}^{n} \lambda^{\alpha,i}{}_p e^\alpha{}_i, \qquad 1 \leqq p \leqq m;$$

the $\lambda^{\alpha,i}{}_p$, $1 \leqq i \leqq n$, $1 \leqq p \leqq m$, are regular functions on U_α, and our assumption that $\mathrm{Im}[\psi]$ is not the zero sheaf means that for any $\alpha \in J$, not all of the functions $\lambda^{\alpha,i}{}_p$ are equal to the function zero.

$\pi_G{}^{-1}(U_\alpha)$, the portion of $\mathcal{B}(G)$ over U_α, is a product variety $U_\alpha \times P'_\alpha$, where P'_α is a projective space of dimension $m-1$. Let $\omega^\alpha{}_1, \cdots, \omega^\alpha{}_m$ be the homogeneous coordinate system on P'_α which is paired with $g^\alpha{}_1, \cdots, g^\alpha{}_m$ over U_α with reference to $\mathcal{B}(G)$; let $U'_{\alpha,p}$ denote the open subset on $U_\alpha \times P'_\alpha$ consisting of all points $\mathfrak{g}$ which satisfy $\omega^\alpha{}_p(\mathfrak{g}) \neq 0$; the family $\{U'_{\alpha,p}\}_{\alpha \in J, 1 \leqq p \leqq m}$ forms an open covering of $\mathcal{B}(G)$. The restriction of the basic sheaf $B(G)$ to any $U'_{\alpha,p}$ is a free sheaf of dimension generated by the section $G[\alpha, p]$ of $B(G)$ over $U'_{\alpha,p}$. On $U'_{\alpha,p} \cap U'_{\beta,q}$, we have the transition law

$$G[\alpha, p] = \Big(\sum_{s=1}^{m} G^\beta{}_s{}^\alpha{}_p \omega^\beta{}_s / \omega^\beta{}_q\Big) G[\beta, q].$$

Consider the subset $Y(\psi)$ on the product variety $\mathcal{B}(E) \times \mathcal{B}(G)$ consisting of all points $(\mathfrak{e}, \mathfrak{g})$ such that $\pi_E(\mathfrak{e}) = {}_G\pi(\mathfrak{g})$; $Y(\psi)$ is a non-singular subvariety on $\mathcal{B}(E) \times \mathcal{B}(G)$ of dimension $r+n+m-2$ $(\dim. X = r)$. Let Σ_ψ denote the rational transformation from $Y(\psi)$ onto X which maps a point $(\mathfrak{e}, \mathfrak{g})$ of $Y(\psi)$ onto the point $\mathfrak{p} = \pi_E(\mathfrak{e}) = \pi_G(\mathfrak{g})$ of X; Σ_ψ is a regular mapping from $Y(\psi)$ onto X. The open set $\Sigma_\psi^{-1}(U_\alpha)$ on $Y(\psi)$, consisting of all points which Σ_ψ maps onto U_α, the the product variety $U_\alpha \times P_\alpha \times P'_\alpha$.

We shall say that a point $\mathfrak{e}$ on $U_\alpha \times P_\alpha$ satisfies the requirement (R) if:

(R) $\sum_{i=1}^{n} \lambda^{\alpha,i}{}_p(\mathfrak{p})\tau^\alpha{}_i(\mathfrak{e}) \neq 0$ for at least one p, $1 \leqq p \leqq m$; $\lambda^{\alpha,i}{}_p(\mathfrak{p})$ is the value of $\lambda^{\alpha,i}{}_p$ at the point $\mathfrak{p} = \pi_E(\mathfrak{e})$. The points of $U_\alpha \times P_\alpha$ which fail to satisfy (R) form a proper algebraic subset on $U_\alpha \times P_\alpha$ since $\operatorname{Im}[\psi]$ is not the sheaf zero. Let T_α be the closed (i.e., algebraic) set on $U_\alpha \times P_\alpha \times P'_\alpha$ consisting of all points such that

$$\rho_0 \omega^\alpha{}_p(\mathfrak{g}) = \rho_1 \sum_{i=1}^{n} \lambda^{\alpha,i}{}_p(\mathfrak{p})\tau^\alpha{}_i(\mathfrak{e}), \qquad 1 \leqq p \leqq m;$$

ρ_0, ρ_1 are arbitrary constants not both zero, and $\mathfrak{p} = \Sigma_\psi(\mathfrak{e}, \mathfrak{g})$; T_α is a proper algebraic subset on $U_\alpha \times P_\alpha \times P'_\alpha$. If $\mathfrak{e}$ satisfies (R), then there is a unique point $\mathfrak{g}$ on $U_\alpha \times P'_\alpha$ such that $(\mathfrak{e}, \mathfrak{g})$ is a point T_α. Consequently, there is a unique subvariety V_α of dimension $r+n-1$ on $U_\alpha \times P_\alpha \times P'_\alpha$ which is a maximal component of T_α, and with the property that V_α contains all points $(\mathfrak{e}, \mathfrak{g})$ on T_α such that $\mathfrak{e}$ satisfies (R). Let η_α be that rational transformation from $U_\alpha \times P_\alpha$ into $U_\alpha \times P'_\alpha$ whose graph is V_α. It is easy to check that the restriction of η_α to $\pi_E^{-1}(U_\alpha \cap U_\beta)$ is equal to the restriction of η_β to $\pi_E^{-1}(U_\alpha \cap U_\beta)$; hence there is a unique rational transformation $\mathcal{B}(\psi)$ from $\mathcal{B}(E)$ into $\mathcal{B}(G)$ whose restriction to any $U_\alpha \times P_\alpha$ is equal to η_α. The reqiurement (R) is a sufficient condition for $\mathcal{B}(\psi)$ to be a regular at a point $\mathfrak{e}$; but in general, it is not a necessary condition.

Consider the subvariety $\mathcal{G}(\psi)$ on $Y(\psi)$ which is the graph of $\mathcal{B}(\psi)$; thet family $\{V_\alpha\}$ forms a covering of $\mathcal{G}(\psi)$ by open sets. Let $\psi_{;1}$ and $\psi_{;2}$ denote the projections from $\mathcal{G}(\psi)$ into $\mathcal{B}(E)$ and $\mathcal{B}(G)$ respectively; $\psi_{;1}B(E)$ and $\psi_{;2}B(G)$ are locally free sheaves of dimension one defined on $\mathcal{G}(\psi)$, for they are the reciprocal images of $B(E)$ and $B(G)$ with respect to $\psi_{;1}$ and $\psi_{;2}$ respectively. We shall exhibit a canonical homomorphism $B(\psi)$ of the sheaf $\psi_{;2}B(G)$ into $\psi_{;1}B(E)$; $B(\psi)$ is called the basic homomorphism associated with the sheaf homomorphism $\psi\colon G \to E$.

The restriction of $\psi_{;1}B(E)$, resp. $\psi_{;2}B(G)$, to $\psi_{;1}(U_{\alpha,i})$, resp. $\psi_{;2}(U'_{\alpha,p})$,

is a free sheaf of dimension one generated by the section $\psi_{;1}^{-1}E[\alpha, i]$, resp. $\psi_{;2}^{-1}G[\alpha, p]$, which is the reciprocal image of the section $E[\alpha, i]$, resp. $G[\alpha, p]$; (we consider here only those $U'_{\alpha,p}$ such that $\psi_{;2}^{-1}(U'_{\alpha,p})$ is non-empty). We have the transition laws

$$\psi_{;1}^{-1}E[\alpha, i] = \left(\sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{i}(\tau^{\beta}{}_{h}/\tau^{\beta}{}_{j})\right)\psi_{;1}^{-1}E[\beta, j]$$

on $\psi_{;1}^{-1}(U_{\alpha,i} \cap U_{\beta,j})$, and

$$\psi_{;2}^{-1}G[\alpha, p] = \left(\sum_{s=1}^{m} G^{\beta}{}_{s}{}^{\alpha}{}_{p}(\omega^{\beta}{}_{s}/\omega^{\beta}{}_{q})\right)\psi_{;2}^{-1}G[\beta, q]$$

on $\psi_{;2}^{-1}(U'_{\alpha,p} \cap U'_{\beta,q})$; the coefficients in these transition laws are to be viewed as rational functions on $\mathcal{B}(\psi)$. For each triple $(\alpha; i, p)$, $\alpha \in J$, $1 \leqq i \leqq n$, $1 \leqq p \leqq m$, such that $\psi_{;1}^{-1}(U_{\alpha,i}) \cap \psi_{;2}^{-1}(U'_{\alpha,p})$ is non-empty, we set

$$U_{\alpha;i,p} = \psi_{;1}^{-1}(U_{\alpha,i}) \cap \psi_{;2}^{-1}(U'_{\alpha,p});$$

the family of all such admissible sets forms an open covering of $\mathcal{B}(\psi)$. The homomorphism $B(\psi)$ is constructed according to the rule that its restriction to any $U_{\alpha;i,p}$ is described by

$$\psi_{;2}^{-1}G[\alpha, p] \to \left(\sum_{h=1}^{n} \lambda^{\alpha,h}{}_{p}(\tau^{\alpha}{}_{h}/\tau^{\alpha}{}_{i})\right)\psi_{;1}^{-1}E[\alpha, i];$$

the coefficient is viewed as a regular function on $U_{\alpha;i,p}$. It is easy to verify that $B(\psi)$ has been constructed in a consistent way.

There is also a naturally determined locally free sheaf $S(\psi)$ of dimension one defined on $\mathcal{B}(\psi)$, and a naturally determined isomorphism of the product sheaf $(\psi_{;2}^{-1}B(G)) \otimes S(\psi)$ onto the sheaf $\psi_{;1}^{-1}B(E)$. The restriction of $S(\psi)$ to any $U_{\alpha;i,p}$ is a free sheaf of dimension one generated by a section $S[\alpha; i, p]$, and we have the transition law

$$S[\alpha; i, p] = \left(\sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{i}(\tau^{\beta}{}_{h}/\tau^{\beta}{}_{j})\right)\left(\sum_{s=1}^{m} G^{\beta}{}_{s}{}^{\alpha}{}_{p}(\omega^{\beta}{}_{s}/\omega^{\beta}{}_{p})\right)^{-1} S[\beta; j, q]$$

on $U_{\alpha;i,p} \cap U_{\beta;j,q}$; the restriction of the isomorphism to any $U_{\alpha;i,p}$ is described by

$$(\psi_{;2}^{-1}G[\alpha, p]) \otimes S[\alpha; i, p] \to \psi_{;1}^{-1}E[\alpha; i, p].$$

Everything is consistent since we have

$$\begin{aligned}&\left(\sum_{h=1}^{n} \lambda^{\alpha,h}{}_{p}(\tau^{\alpha}{}_{h}/\tau^{\alpha}{}_{i})\right)\\ &\qquad = \left(\sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{i}(\tau^{\beta}{}_{h}/\tau^{\beta}{}_{j})\right)^{-1}\left(\sum_{s=1}^{m} G^{\beta}{}_{s}{}^{\alpha}{}_{p}(\omega^{\beta}{}_{s}/\omega^{\beta}{}_{q})\right)\left(\sum_{h=1}^{n} \lambda^{\beta,h}{}_{q}(\tau^{\beta}{}_{h}/\tau^{\beta}{}_{j})\right)\end{aligned}$$

on $U_{\alpha;i,p} \cap U_{\beta;j,q}$.

§ 17. Assume that ψ maps G onto E. It is permissible to suppose, on the basis of the definition of a coherent locally free sheaf together with Lemma 2 of § 14, that the families of generating section for E and G have been chosen such that the restriction of ψ to any U_α is described by

$$g^\alpha{}_i \to e^\alpha{}_i, \qquad 1 \leqq i \leqq n,$$

$$g^\alpha{}_{n+u} \to 0, \qquad 1 \leqq u \leqq m-n.$$

In this situation, $\mathcal{B}(\psi)$ is a bi-regular mapping from $\mathcal{B}(E)$ into $\mathcal{B}(G)$; a point $\mathfrak{e}$ on $U_\alpha \times P_\alpha$ is mapped by $\mathcal{B}(\psi)$ onto the point $\mathfrak{g}$ on $U_\alpha \times P'_\alpha$ such that

$$\pi_G(\mathfrak{g}) = \pi_E(\mathfrak{e}),$$

$$\omega^\alpha{}_i(\mathfrak{g}) = \tau^\alpha{}_i(\mathfrak{g}), \qquad 1 \leqq i \leqq n,$$

$$\omega^\alpha{}_{n+u}(\mathfrak{g}) = 0, \qquad 1 \leqq u \leqq m-n.$$

We view $\mathcal{B}(E)$ as subvariety $\mathcal{B}(G)$ by the device of identifying $\mathcal{B}(E)$ with its image with respect to $\mathcal{B}(\psi)$. If $p > n$, then $\mathcal{B}(E) \cap U'_{\alpha,p}$ is empty. For any i, $1 \leqq i \leqq n$, the $m-n$ functions

$$\omega^\alpha{}_{n+u}/\omega^\alpha{}_i, \qquad 1 \leqq u \leqq m-n,$$

generate the ideal determined by $\mathcal{B}(E)$ in the local ring of $\mathcal{B}(G)$ at every point on $U'_{\alpha,i}$.

We have that

$$G^\beta{}_i{}^\alpha{}_j = E^\beta{}_i{}^\alpha{}_j, \qquad 1 \leqq i, j \leqq n,$$

$$G^\beta{}_p{}^\alpha{}_q = 0, \qquad 1 \leqq p \leqq n, n+1 \leqq q \leqq m-n;$$

which is to say, we have the transition laws

$$g^\alpha{}_j = \sum_{i=1}^{n} E^\beta{}_i{}^\alpha{}_j g^\beta{}_i + \sum_{u=1}^{m-n} G^\beta{}_{n+u}{}^\alpha{}_j g^\beta{}_{n+u}$$

for $1 \leqq j \leqq n$,

$$g^\alpha{}_{n+v} = \sum_{u=1}^{m-n} G^\beta{}_{n+u}{}^\alpha{}_{n+v} g^\beta{}_{n+u}$$

for $1 \leqq v \leqq m-n$. It is an immediate conseqence of these transition laws, together with the fact that the functions

$$\omega^\alpha{}_{n+u}/\omega^\alpha{}_i, \qquad 1 \leqq u \leqq m-n,$$

generate the ideal determined by $\mathcal{B}(E)$ on $U'_{\alpha,i}$, that the induced sheaf of $B(G)$ on $\mathcal{B}(E)$ is equal to $B(E)$.

Thus, under the assumption that ψ maps G onto E, we have that $\mathcal{B}(\psi)$

is a bi-regular mapping of $\mathfrak{B}(E)$ onto a subvariety on $\mathfrak{B}(G)$; if we identify $\mathfrak{B}(E)$ with that subvariety, then the restriction of π_G to $\mathfrak{B}(E)$ is equal to π_E, and the induced sheaf of $B(G)$ on $\mathfrak{B}(E)$ is equal to $B(E)$; in particular, the trace of the divisor class $\Theta(G)$ on $\mathfrak{B}(E)$ is equal to $\Theta(E)$.

Suppose that $m > n$. The sheaf $\mathrm{Ker}[\psi]$ is a locally free sheaf of dimension $m-n$ defined on X; the restriction of $\mathrm{Ker}[\psi]$ to any U_α is the free sheaf generated by the sections $g^\alpha{}_{n+1}, \cdots, g^\alpha{}_m$, and we have the transition laws

$$g^\alpha{}_{n+v} = \sum_{u=1}^{m-n} H^\beta{}_u{}^\alpha{}_v g^\beta{}_{n+u}, \qquad 1 \leqq v \leqq m-n,$$

with

$$H^\beta{}_u{}^\alpha{}_v = G^\beta{}_{n+u}{}^\alpha{}_{n+v}, \qquad 1 \leqq u, v \leqq m-n.$$

We construct a locally free sheaf H of dimension $m-n$ defined on X as follows: the restriction of H to U_α is a free sheaf generated by sections $h^\alpha{}_1, \cdots, h^\alpha{}_{m-n}$, and we have the transition laws

$$h^\alpha{}_v = \sum_{u=1}^{m-n} H^\beta{}_u{}^\alpha{}_v h^\beta{}_u, \qquad 1 \leqq v \leqq m-n.$$

We construct an isomorphism θ from H into G according to the rule: the restriction of θ to U_α is described by

$$\theta \colon h^\alpha{}_u \to g^\alpha{}_{n+u}, \qquad 1 \leqq u \leqq m-n;$$

the sheaf $\mathrm{Im}[\theta]$ is equal to $\mathrm{Ker}[\psi]$, but we must emphasize that the range of θ is the sheaf G; consequently, there is the exact sequence

$$0 \to H \xrightarrow{\theta} G \xrightarrow{\psi} E \to 0$$

of locally free sheaves defined on X.

We shall examine the constructions of § 16 with refernce to the homomorphism $\theta \colon H \to G$. $\pi_H{}^{-1}(U_\alpha)$, the portion of $\mathfrak{B}(H)$ over U_α, is a product variety $U_\alpha \times P''_\alpha$; P''_α is a projective space of dimension $m-n-1$ with a homogeneous coordinate system $\eta^\alpha{}_1, \cdots, \eta^\alpha{}_{m-n}$ which is paired with the sections $h^\alpha{}_1, \cdots, h^\alpha{}_{m-n}$ over U_α with reference to the construction of $\mathfrak{B}(H)$. $U''_{\alpha,u}$, $1 \leqq u \leqq m-n$, is the open set on $U_\alpha \times P''_\alpha$ consisting of all points $\mathfrak{h}$ such that $\eta^\alpha{}_u(\mathfrak{h}) \neq 0$; the restriction of the basic sheaf $B(H)$ to $U''_{\alpha,u}$ is a free sheaf of dimension one generated by the section $H[\alpha, u]$; we have the transition law

$$H[\alpha, u] = \Big(\sum_{s=1}^{m-n} H^\beta{}_s{}^\alpha{}_u (\eta^\beta{}_s / \eta^\beta{}_v)\Big) H[\beta, v]$$

on $U''_{\alpha,u} \cap U''_{\alpha,v}$.

$Y(\theta)$ is the non-singular subvariety on $\mathscr{B}(G)\times\mathscr{B}(H)$ consisting of all points $(\mathfrak{g},\mathfrak{h})$ such that

$$\pi_G(\mathfrak{g})=\pi_H(\mathfrak{h})\,;$$

Σ_θ is the projection from $Y(\theta)$ onto X which maps a point $(\mathfrak{g},\mathfrak{h})$ onto the point $\pi_G(\mathfrak{g})=\pi_H(\mathfrak{h})=\mathfrak{p}$ on X; $\Sigma_\theta^{-1}(U_\alpha)$ is the product variety $U_\alpha\times P'_\alpha\times P''_\alpha$. Let $(\mathfrak{g},\mathfrak{h})$ be a point on $\mathscr{E}(\theta)\cap\Sigma_\theta^{-1}(U_\alpha)$, and suppose that $\eta^\alpha_{u_0}(\mathfrak{h})\neq 0$, $\omega^\alpha_{p_0}(\mathfrak{g})\neq 0$. We shall prove that $(\mathfrak{g},\mathfrak{h})$ is a simple point on $\mathscr{E}(\theta)$.

Case I: $p_0>n$. The $m-n-1$ functions

$$\omega^\alpha_{n+u}/\omega^\alpha_{p_0'}-\eta^\alpha_u/\eta^\alpha_{n_0}, \qquad u\neq p_0-n,\ 1\leqq n\leqq m-n,$$

generate the ideal determined by $\mathscr{E}(\theta)$ in the local ring of $Y(\theta)$ at $(\mathfrak{g},\mathfrak{h})$; visibly, $(\mathfrak{g},\mathfrak{h})$ is a simple point on $\mathscr{E}(\theta)$ and $\theta_{;1}$, the projection from $\mathscr{E}(\theta)$ onto $\mathscr{B}(G)$, bi-regularly maps some open neighborhood of $(\mathfrak{g},\mathfrak{h})$ on $\mathscr{E}(\theta)$ onto an open neighborhood of $\mathfrak{g}$ on $\mathscr{B}(G)$; in fact, the restriction of $\theta_{;1}$ to $\theta_{;1}^{-1}(U'_{\alpha,p_0})$ is a bi-regular map of that open set onto U'_{α,p_0}.

Case II: $\omega^\alpha_p(\mathfrak{g})=0$ for all $n<p\leqq m$, so that $\omega^\alpha_{i_0}(\mathfrak{g})\neq 0$ for some i_0, $1\leqq i_0\leqq n$. In this case, the $m-n-1$ functions

$$\omega^\alpha_{n+u}/\omega^\alpha_{i_0}-(\eta^\alpha_u/\eta^\alpha_{u_0})\,\omega^\alpha_{n+u_0}/\omega^\alpha_{i_0}, \qquad u\neq u_0,\ 1\leqq u\leqq m-n,$$

generate the ideal determined by $\mathscr{E}(\theta)$ in the local ring at $Y(\theta)$ at $(\mathfrak{g},\mathfrak{h})$; visibly, $(\mathfrak{g},\mathfrak{h})$ is a simple point on $\mathscr{E}(\theta)$; moreover, the variety $\theta_{;1}^{-1}(U'_{\alpha,i_0})$ is obtained from monoidal transformation of U'_{α,i_0} centered on the subvariety $\mathscr{B}(E)\cap U'_{\alpha,i_0}$, since the ideal determined by that subvariety is generated by the functions

$$\omega^\alpha_{n+u}/\omega^\alpha_{i_0}, \qquad 1\leqq u\leqq m-n,$$

in the local ring at every point on U'_{α,i_0}.

Thus the projection $\theta_{;1}$ is an anti-monoidal transformation from $\mathscr{E}(\theta)$ onto $\mathscr{B}(G)$; the center is the subvariety $\mathscr{B}(E)$ on $\mathscr{B}(G)$. Let $U'_{\alpha;p_0,u_0}$, $\alpha\in J$, $1\leqq p_0\leqq m$, $1\leqq u_0\leqq m-n$, denote the open subset on $\mathscr{E}(\theta)$ consisting of all points $(\mathfrak{g},\mathfrak{h})$ on $\mathscr{E}(\theta)\cap\Sigma_\theta^{-1}(U_\alpha)$ which satisfy

$$\omega^\alpha_{p_0}(\mathfrak{g})\neq 0, \qquad \eta^\alpha_{n_0}(\mathfrak{h})\neq 0\,;$$

let $\mathscr{N}_\theta$ denote the anti-center of $\theta_{;1}$. Then $\mathscr{N}_\theta\cap U'_{\alpha;p_0,u_0}$ is empty for $n<p_0\leqq m$, and for $p_0=i_0$, $i_0\leqq n$, the function

$$\omega^\alpha_{n+u_0}/\omega^\alpha_{i_0}$$

generates the ideal determined by $\mathfrak{N}_\theta$ in the local ring of $\mathcal{B}(\theta)$ at every point on $U'_{\alpha;p_0,u_0}$. From the previous discussion on monoidal transformations, we know that the restriction of $\theta_{;1}$ to $\mathfrak{N}_\theta$ equips that variety with the sttructure of a projecive fiber bundle whose base space is $\mathfrak{B}(E)$ and whose fiber is a projective space of dimension $m-n-1$; as such, $\mathfrak{N}_\theta$ is the dual projective bundle of the sheaf $N(\mathfrak{B}(G), \mathfrak{B}(E))$ of germs of covariant normal vectors fields to $\mathfrak{B}(E)$ in $\mathfrak{B}(G)$; the restriction of $\theta_{;1}$ to $\mathfrak{N}_\theta$ is equal to the bundle projection π_N $(\pi_N = \pi_{N(\mathfrak{B}(G);\mathfrak{B}(E))})$ of $\mathfrak{N}_\theta$ onto $\mathfrak{B}(E)$.

We have that

$$\omega^\alpha{}_{n+u}/\omega^\alpha{}_{i_0} = (\sum_{t=1}^{m-n} H^\beta{}_t{}^\alpha{}_u (\omega^\beta{}_{n+t}/\omega^\beta{}_{i_1}))(\sum_{s=1}^{m} G^\beta{}_s{}^\alpha{}_{i_0}(\omega^\beta{}_s/\omega^\beta{}_{i_1}))^{-1}$$

on $U'_{\alpha,i_0} \cap U'_{\beta,i_1}$ for all $1 \leqq u \leqq m-n$, where i_0, i_1 are fixed and $\mathrm{v} \leqq i_0, i_1 \leqq n$. Consequently, the restriction of $N(\mathfrak{B}(G); \mathfrak{B}(E))$ to any $U_{\alpha,i}$ $(1 \leqq i \leqq n)$ is a free sheaf of dimension $r-n$ generated by sections

$$z^{\alpha,i}{}_1, \cdots, z^{\alpha,i}{}_1,$$

and we have the transition laws

$$z^{\alpha,i}{}_u = (\sum_{s=1}^{n} E^\beta{}_s{}^\alpha{}_i(\omega^\beta{}_s/\omega^\beta{}_j))^{-1} \sum_{t=1}^{m-n} H^\beta{}_t{}^\alpha{}_u z^{\beta,j}{}_t$$

on $U_{\alpha,i} \cap U_{\beta,j}$ for all $1 \leqq u \leqq m-n$, since we have

$$E^\beta{}_s{}^\alpha{}_i = G^\beta{}_s{}^\alpha{}_i \qquad 1 \leqq i, s \leqq n,$$

and $\omega^\beta{}_s/\omega_{\beta j}$ is the rational function zero on $U_{\alpha,i} = \mathfrak{B}(E) \cap U'_{\alpha,i}$ for $s > n$. By inspection, we obtain

$$N(\mathfrak{B}(G); \mathfrak{B}(E)) = B^{-1}(E) \otimes \pi_E H;$$

which is to say, the right hand side is the product sheaf of $B^{-1}(E)$ (where $B^{-1}(E) \otimes B(E) = \mathcal{O}_{\mathfrak{B}(E)}$) with the reciprocal image $\pi_E H$ of the sheaf H with respect to the mapping π_E: $\mathfrak{B}(E) \to X$.

Appealing to the constructions of § 16, we have the locally free sheaf $S(\theta)$ of dimension one defined on $\mathcal{B}(\theta)$ with the property

$$\theta_{;2}B(H) \otimes S(\theta) = \theta_{;1}B(G);$$

the sheaf $\theta_{;1}B(G)$, resp. $\theta_{;2}B(H)$, is the reciprocal image of $B(G)$, resp. $B(H)$, with respect to the mapping $\theta_{;1}$, resp. $\theta_{;2}$. The basic class $\circledcirc(S(\theta))$ of $S(\theta)$ is the divisor class of the divisor $\mathfrak{N}_\theta$ on $\mathcal{B}(\theta)$; this follows from the fact that

$$\omega^\alpha{}_{n+u}/\omega^\alpha{}_i = (\sum_{t=1}^{m-n} H^\beta{}_t{}^\alpha{}_u(\eta^\beta{}_t/\eta^\beta{}_v))(\sum_{s=1}^{m} G^\beta{}_s{}^\alpha{}_i \omega^\beta{}_s/\omega^\beta{}_j)^{-1} \omega^\beta{}_{n+v}/\omega^\beta{}_j$$

on $U'_{\alpha;i,u} \cap U'_{\beta;j,v}$ for fixed i, j, u, v, $1 \leqq i, j \leqq n$, $1 \leqq u, v \leqq m-n$, and the transition law

$$S[\alpha;i,u] = \Big(\sum_{t=1}^{m-n} H^{\beta}{}_{t}{}^{\alpha}{}_{n}(\eta^{\beta}{}_{t}/\eta^{\beta}{}_{v})\Big)^{-1}\Big(\sum_{s=1}^{m} G^{\beta}{}_{s}{}^{\alpha}{}_{i}\omega^{\beta}{}_{s}/\omega^{\beta}{}_{j}\Big) S[\beta;j,v]$$

on $U'_{\alpha;i,u} \cap U'_{\beta;j,v}$. By inspection, we obtain that the induced sheaf of $S(\theta)$ on the subvariety $\mathfrak{N}_\theta$ is the sheaf $B^{-1}(N(\mathcal{B}(G);\mathcal{B}(E)))$. We have arrived at the important formula

$$\theta_{;2}{}^*(\Theta(H)) + \Theta(S(\theta)) = \theta_{;1}{}^*(\Theta(G));$$

$\theta_{;1}{}^*(\Theta(G))$, resp. $\theta_{;2}{}^*(\Theta(H))$, is the reciprocal image of the basic divisor class $\Theta(G)$, resp. $\Theta(H)$, with respect to the projection $\theta_{;1}$, resp. $\theta_{;2}$, and $\Theta(S(\theta))$ is the divisor class of the anti-center $\mathfrak{N}_\theta$ of $\theta_{;1}$.

We shall prove that the projection $\theta_{;2}$ equips $\mathcal{B}(\theta)$ with the structure of a projective fiber bundle whose base space is $\mathcal{B}(H)$; as such $\mathcal{B}(\theta)$ is the dual projective bundle of a certain locally free sheaf $R(\theta)$ of dimension $n+1$ defined on $\mathcal{B}(H)$. Let $\mathfrak{h}$ be a point on U''_{α,u_0}. $\theta_{;2}{}^{-1}(\mathfrak{h})$ consists of all points $(\mathfrak{g},\mathfrak{h})$ such that $\mathfrak{g} \in U_\alpha \times P'_\alpha$ satisfies

(a) $\pi_G(\mathfrak{g}) = \pi_H(\mathfrak{h})$

(b) $\omega^{\alpha}{}_{n+u}(\mathfrak{g}) - (\eta^{\alpha}{}_{u}/\eta^{\alpha}{}_{u_0}(\mathfrak{h}))\omega^{\alpha}{}_{n+u_0}(\mathfrak{g}) = 0$, $u \neq u_0, 1 \leqq u \leqq m-n$;

consequently, $\theta_{;2}{}^{-1}(U''_{\alpha,u_0})$ is the product variety of U''_{α,u_0} with a projective subspace of dimension n on P'_α; this subspace is described by the equations

$$\omega^{\alpha}{}_{n+u} - (\eta^{\alpha}{}_{u}/\eta^{\alpha}{}_{u_0})\omega^{\alpha}{}_{n+u_0} = 0, \qquad u \neq u_0, 1 \leqq u \leqq m-n.$$

If the point $(\mathfrak{g},\mathfrak{h})$ belongs to $\theta_{;2}{}^{-1}(U''_{\alpha,u_0}) \cap \theta_{;2}{}^{-1}(U''_{\beta,v_0})$, then we have (where $\mathfrak{p} = \pi_H(\mathfrak{h}) = \pi_G(\mathfrak{g})$)

$$\omega^{\alpha}{}_{i}(\mathfrak{g}) = \rho\Big(\sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{i}(\mathfrak{p})\omega^{\beta}{}_{h}(\mathfrak{g}) + \Big(\sum_{t=1}^{m-n} G^{\beta}{}_{n+t}{}^{\alpha}{}_{i}(\mathfrak{p})\eta^{\beta}{}_{t}/\eta^{\beta}{}_{v_0}(\mathfrak{h})\Big)\omega^{\beta}{}_{n+v_0}(\mathfrak{g})\Big),$$

for all $1 \leqq i \leqq n$, and

$$\omega^{\alpha}{}_{n+u_0}(\mathfrak{g}) = \rho\Big(\sum_{t=1}^{m-n} H^{\beta}{}_{t}{}^{\alpha}{}_{u_0}(\mathfrak{p})\eta^{\beta}{}_{t}/\eta^{\beta}{}_{v_0}(\mathfrak{h})\Big)\omega^{\beta}{}_{n+v_0}(\mathfrak{g});$$

this proves that $\theta_{;2}$ equips $\mathcal{B}(\theta)$ with the structure of a projective fiber bundle.

$R(\theta)$ is a locally free sheaf of dimension $n+1$ defined on $\mathcal{B}(H)$ as follows: the restriction of $R(\theta)$ to U''_{α,u_0} ($\alpha \in J$, $1 \leqq u_0 \leqq m-n$) is a free sheaf of dimension $n+1$ generated by sections

$$r_1[\alpha,u_0], \cdots, r_n[\alpha,u_0], r_{n+1}[\alpha,u_0]$$

on $U''_{\alpha,u_0} \cap U''_{\beta,v_0}$; there is the transition law

$$r_i[\alpha, u_0] = \sum_{h=1}^{n} E^{\beta}{}_{h}{}^{\alpha}{}_{i} r_h[\beta, v_0] + \left(\sum_{t=1}^{m-n} G^{\beta}{}_{n+t}{}^{\alpha}{}_{i}(\eta^{\beta}{}_{t}/\eta^{\beta}{}_{v_0})\right) r_{n+1}[\beta, v_0]$$

for $1 \leqq i \leqq n$, and

$$r_{n+1}[\alpha, u_0] = \left(\sum_{t=1}^{m-n} H^{\beta}{}_{t}{}^{\alpha}{}_{u_0}(\eta^{\beta}{}_{t}/\eta^{\beta}{}_{v_0})\right) r_{n+1}[\beta, v_0].$$

We identify the dual projective bundle of the sheaf $R(\theta)$ with $\mathcal{E}(\theta)$ according to the rule that the homogeneous coordinates

$$\omega^{\alpha}{}_{1}, \cdots, \omega^{\alpha}{}_{n}, \omega^{\alpha}{}_{n+u_0}$$

are paired with the sections

$$r_1[\alpha, u_0], \cdots, r_n[\alpha, u_0], r_{n+1}[\alpha, u_0]$$

over U''_{α,u_0} with reference to the construction of $\mathcal{B}(R(\theta))$; the projection $\theta_{;2}$ is then equal to the bundle projection $\pi_{R(\theta)}$. There is an evident isomorphism of $B(H)$ into $R(\theta)$; the restriction of this isomorphism to any U''_{α,u_0} is described by

$$H[\alpha, u_0] \to r_{n+1}[\alpha, u_0].$$

It follows by inspection that the quotient sheaf of $R(\theta)$ modulo the image of $B(H)$ is isomorphic to the sheaf $\pi_H E$, the reciprocal image of E with respect to the mapping π_H. Thus we have the exact sequence

$$0 \to B(H) \to R(\theta) \to \pi_H E \to 0$$

of locally free sheaves defined on $\mathcal{B}(H)$.

The homomrophism from $R(\theta)$ onto $\pi_H E$ permits us to identity $\mathcal{B}(\pi_H E)$ with a subvariety on $\mathcal{E}(\theta)$ in such a fashion that the restriction of $\theta_{;2}$ to $\mathcal{B}(\pi_H E)$. More precisely, we can assert that $\mathcal{B}(\pi_H E)$, as a subvariety on $\mathcal{E}(\theta)$, is equal to the previously introduced variety $\mathfrak{N}_{\theta}$. For the restriction to U''_{α,u_0} of our homomorphism from $R(\theta)$ onto $\pi_H E$ is described by

$$r_i[\alpha, u_0] \to \pi_H{}^{-1} e^{\alpha}{}_{i}, \qquad 1 \leqq i \leqq n,$$

$$r_{n+1}[\alpha, u_0] \to 0,$$

where $\pi_H{}^{-1} e^{\alpha}{}_{i}$ is the reciprocal image of the section $e^{\alpha}{}_{i}$; consequently, $\mathcal{B}(\pi_H E) \cap \theta_{;2}{}^{-1}(U''_{\alpha,u_0})$ consists of all points $(\mathfrak{g}, \mathfrak{h})$ which satisfy

$$\omega^{\alpha}{}_{n+u_0}(\mathfrak{g}) = 0,$$

which clearly gives us that $\mathcal{B}(\pi_H E) \cap \theta_{;2}{}^{-1}(U''_{\alpha,u_0})$ is identical to

$$\mathfrak{N}_{\theta} \cap \theta_{;2}{}^{-1}(U''_{\alpha,u_0}).$$

Thus the subvariety $\mathfrak{N}_\theta$ on $\mathcal{B}(\theta)$ carries the structure of a projective fiber bundle in two ways; the restriction of $\theta_{;2}$ to $\mathfrak{N}_\theta$ equips $\mathfrak{N}_\theta$ with the structure of $\mathcal{B}(\pi_H E)$, and the restriction of $\theta_{;1}$ to $\mathfrak{N}_\theta$ equips $\mathfrak{N}_\theta$ with the structure of $\mathcal{B}(\pi_E H)$— since $N(\mathcal{B}(G), \mathcal{B}(E)) = \pi_E H \otimes B^{-1}(E)$.

It is a straightforward matter to check that

$$B(R(\theta)) = \theta_{;1} B(G);$$

the restriction of $\theta_{;1}B(G)$ to $\mathfrak{N}_\theta$ is equal to the reciprocal image of $B(E)$ with respect to the mapping from $\mathfrak{N}_\theta$ onto $\mathcal{B}(E)$ which is the restriction of $\theta_{;1}$ to $\mathfrak{N}_\theta$.

§ 18. Let V be a non-singular subvariety of dimension $r-1$ on X ($\dim. X = r$). E and G are locally free sheaves defined on X as in § 16; but here we assume that ψ is an isomorphism from G into E, and that the residue class sheaf Q of E modulo the image of G by ψ is the extension to X of a locally free sheaf defined on V which we continue to denote as Q. We suppose that the covering $\{U_\alpha\}_{\alpha\in J}$ of X has the property that for each α, there exists a regular function x^α on U_α which generates the ideal determined by V in the local ring of X at each point on U_α, and that the restriction of Q to $V \cap U_\alpha$ (assuming that $V \cap U_\alpha$ is non-empty) is a free sheaf of dimension q defined on $V \cap U_\alpha$ generated by sections

$$l^\alpha{}_1, \cdots, l^\alpha{}_q$$

of Q over $V \cap U_\alpha$. It is permissible to suppose that the sections $e^\alpha{}_1, \cdots, e^\alpha{}_n$ are such that the restriction to U_α of the homomorphism from E onto Q is described by

$$\begin{aligned} &e^\alpha{}_i \to l^\alpha{}_i, && 1 \leqq i \leqq q,\\ &e^\alpha{}_{q+u} \to 0, && 1 \leqq u \leqq n-q, \end{aligned}$$

and the restriction of the kernel of this homomorphism to U_α is generated by

$$\begin{aligned} &x^\alpha e^\alpha{}_i \to 0, && 1 \leqq i \leqq q,\\ &e^\alpha{}_{q+u} \to 0, && 1 \leqq u \leqq n-q; \end{aligned}$$

furthermore, we can suppose that the sections $g^\alpha{}_1, \cdots, g^\alpha{}_n$ (here we must have $m = n$) are such that the restriction of ψ to U_α is described by

$$\begin{aligned} &g^\alpha{}_i \to x^\alpha e^\alpha{}_i, && 1 \leqq i \leqq q,\\ &g^\alpha{}_{q+j} \to e^\alpha{}_{q+u}, && 1 \leqq u \leqq n-q. \end{aligned}$$

Thus we have the exact sequence

$$0 \to G \to E \to Q \to 0,$$

where Q is the extension to X of a locally free sheaf defined on V.

We suppose that x^α is the constant function 1 for each α such that $V \cap U_\alpha$ is empty. For each ordered pair, we introduce the function $D^{\beta\alpha}$ according to

$$x^\alpha D^{\beta\alpha} = x^\beta;$$

$D^{\beta\alpha}$ is a regular function on $U_\alpha \cap U_\beta$ which vanishes at no point of $U_\alpha \cap U_\beta$, and we have

$$D^{\alpha\gamma} D^{\alpha\beta} D^{\beta\alpha} = 1,$$
$$D^{\alpha\beta} D^{\beta\alpha} = 1.$$

We have the transition laws

$$e^\alpha{}_i = \sum_{h=1}^{n} E^\beta{}_h{}^\alpha{}_i e^\beta{}_h, \qquad 1 \leqq i \leqq n,$$

$$g^\alpha{}_i = \sum_{h=1}^{n} G^\beta{}_h{}^\alpha{}_i g^\beta{}_h, \qquad 1 \leqq i \leqq n,$$

for E and G respectively; but in view of the homomorphism ψ, we must have

$$G^\beta{}_h{}^\alpha{}_i = (D^{\beta\alpha})^{-1} E^\beta{}_h{}^\alpha{}_i, \qquad 1 \leqq i \leqq q, 1 \leqq h \leqq q,$$
$$G^\beta{}_{q+n}{}^\alpha{}_i = (D^{\beta\alpha})^{-1} x^\beta E^\beta{}_{q+u}{}^\alpha{}_i, \qquad 1 \leqq i \leqq q, 1 \leqq u \leqq n-q,$$
$$x^\beta G^\beta{}_h{}^\alpha{}_{q+v} = E^\beta{}_h{}^\alpha{}_{q+v}, \qquad 1 \leqq h \leqq q, 1 \leqq v \leqq n-q,$$
$$G^\beta{}_{q+n}{}^\alpha{}_{q+v} = E^\beta{}_{q+u}{}^\alpha{}_{q+v}, \qquad 1 \leqq u, v \leqq n-q.$$

This gives the transition laws

$$g^\alpha{}_i = (D^{\beta\alpha})^{-1} \Big(\sum_{h=1}^{q} E^\beta{}_h{}^\alpha{}_i g^\beta{}_h + x^\beta \sum_{u=1}^{n-q} E^\beta{}_{q+u}{}^\alpha{}_i g^\beta{}_{q+u} \Big)$$

for $1 \leqq i \leqq q$, and

$$g^\alpha{}_{q+v} = (x^\beta)^{-1} \sum_{h=1}^{q} E^\beta{}_h{}^\alpha{}_{q+v} g^\beta{}_h + \sum_{u=1}^{n-q} E^\beta{}_{q+u}{}^\alpha{}_{q+v} g^\beta{}_{q+v}$$

for $1 \leqq v \leqq n-q$; in particular, we observe that $(x^\beta)^{-1} E^\beta{}_h{}^\alpha{}_{q+v}$ is a regular function on $U_\alpha \cap U_\beta$ for all $1 \leqq h \leqq q$, $1 \leqq v \leqq n-q$.

Let E', resp. G', denote the induced sheaf of E, resp. G, on the subvariety V; let ψ' denote the induced homomorphism of ψ. E' and G' are locally free sheaves of dimension n defined on V; the induced sheaf of Q on V is clearly the sheaf Q. We have the exact sequence

$$G' \xrightarrow{\psi'} E' \to Q \to 0$$

of locally free sheaves defined on V; but $\operatorname{Ker}[\psi']$ is not the sheaf zero. In fact, the restriction of G' to $V \cap U_\alpha$ (assuming that this is not empty) is a free sheaf of dimension n defined on $V \cap U_\alpha$ and it is generated by the sections $g'^{\alpha}{}_1, \cdots, g'^{\alpha}{}_n$ which are the induced sections of $g^{\alpha}{}_1, \cdots, g^{\alpha}{}_n$ respectively on $V \cap U_\alpha$. The restriction of $\operatorname{Ker}[\psi']$ to $V \cap U_\alpha$ is a free sheaf of dimension q generated by the sections

$$g'^{\alpha}{}_1, \cdots, g'^{\alpha}{}_q;$$

we have the transition laws

$$g'^{\alpha}{}_i = (D'^{\beta\alpha})^{-1} \sum_{h=1}^{q} E'^{\beta}{}_h{}^{\alpha}{}_i g'^{\beta}{}_h, \qquad 1 \leqq h \leqq q,$$

where $D'^{\beta\alpha}$, resp. $E'^{\beta}{}_h{}^{\alpha}{}_i$, is the induced function of $D^{\beta\alpha}$, resp. $E^{\beta}{}_h{}^{c}{}_i$, on $V \cap U_\alpha \cap U_\beta$. On the other hand, we have for the sheaf Q the transition laws

$$l^{\alpha}{}_i = \sum_{h=1}^{q} E'^{\beta}{}_h{}^{\alpha}{}_i l^{\beta}{}_h, \qquad 1 \leqq h \leqq q;$$

this proves that $\operatorname{Ker}[\psi']$ is isomorphic to the product sheaf of Q with a locally free sheaf of dimension one defined on V.

$\mathcal{L}(-V)$ is the sheaf of germs of rational function on X which are multiples of the divisor $-V$ on X. The restriction of $\mathcal{L}(-V)$ to U_α is a free sheaf of dimension one and the function $(x^\alpha)^{-1}$ is a generating section. We have the transition law

$$(x^\alpha)^{-1} = D^{\beta\alpha}(x^\beta)^{-1}$$

on $U_\alpha \cap U_\beta$. It is evident that the basic divisor class $\mathfrak{G}(\mathcal{L}(-V))$ of $\mathcal{L}(-V)$ is the divisor class of V. Let $(\mathcal{L}(-V))'$ denote the induced sheaf of $\mathcal{L}(-V)$ on the subvariety V. Then we obtain by inspection that

$$\operatorname{Ker}[\psi'] \otimes (\mathcal{L}(-V))' = Q,$$

or better,

$$\operatorname{Ker}[\psi'] = Q \otimes (\mathcal{L}(V))',$$

where $(\mathcal{L}(V))'$ is the induced sheaf on V of the sheaf $\mathcal{L}(V)$ of germs of rational functions on X which are multiples of the divisor V. Thus we have obtained the exact sequence

$$0 \to Q \otimes (\mathcal{L}(V))' \to G' \xrightarrow{\psi'} E' \to Q \to 0$$

of locally free sheaves defined on V; this is called the "subordinate exact sequence" of the exact sequence

$$0 \to G \xrightarrow{\psi} E \to Q \to 0.$$

The sheaf $\mathrm{Im}[\psi']$ is a locally free sheaf of dimension $n-q$ defined on V; we denote this sheaf by $M(\psi)$. $M(\psi)$ is a subsheaf of E', and the restriction of $M(\psi)$ to $V\cap U_\alpha$ is a free sheaf generated by the sections

$$e'^{\alpha}_{q+1},\cdots,e'^{\alpha}_{n}.$$

With reference to $M(\psi)$, we have the transition laws

$$e'^{\alpha}_{q+v}=\sum_{u=1}^{n-q}E'^{\beta}{}_{q+u}{}^{\alpha}{}_{q+v}e'_{q+u}, \qquad 1\leqq v\leqq n-q,$$

since $E^{\beta}{}_{h}{}^{\alpha}{}_{q+v}=x^{\beta}G^{\beta}{}_{h}{}^{\alpha}{}_{q+v}$ for $1\leqq h\leqq q$, $1\leqq v\leqq n-q$, which forces $E'^{\beta}{}_{h}{}^{\alpha}{}_{q+v}$ to be the function zero on V. Thus the subordinate exact sequence is composed of the exact sequences

$$0\to Q\otimes(\mathcal{L}(V))'\to G'\to M(\psi)\to 0,$$
$$0\to M(\psi)\to E'\to Q\to 0$$

of locally free sheaves defined on V.

§ 19. Consider the exact sequence

$$0\to G\to E\to Q\to 0$$

of § 18. We shall prove that the graph $\mathcal{G}(\psi)$ of $\mathcal{B}(\psi)$ is a non-singular variety.

We form the variety $Y(\psi)$ and the projection Σ_ψ from $Y(\psi)$ onto X, as in § 16. $\Sigma_\psi^{-1}(U_\alpha)$ is the product variety $U_\alpha\times P_\alpha\times P'_\alpha$. A point $(\mathfrak{e},\mathfrak{g})$ on $\mathcal{G}(\psi)\cap\Sigma_\psi^{-1}(U_\alpha)$ must satisfy

$$\rho_1\omega^{\alpha}{}_{i}(\mathfrak{g})=\rho_2x^{\alpha}(\mathfrak{p})\tau^{\alpha}{}_{i}(\mathfrak{e}), \qquad 1\leqq i\leqq q,$$
$$\rho_1\omega^{\alpha}{}_{q+u}(\mathfrak{g})=\rho_2\tau^{\alpha}{}_{q+u}(\mathfrak{e}), \qquad 1\leqq u\leqq n-q,$$

where $\mathfrak{p}=\Sigma_\psi(\mathfrak{e},\mathfrak{g})=\pi_E(\mathfrak{e})=\pi_G(\mathfrak{g})$. The case where $\mathfrak{p}$ is not a point V is essentially trivial; in fact, we then have that $\mathcal{B}(\psi)$ bi-regularly maps some open neighborhood of $\mathfrak{e}$ on $\mathcal{B}(E)$ onto an open neighborhood of $\mathfrak{g}$ on $\mathcal{B}(G)$. Assume that $\mathfrak{p}$ lies on V so that $x^{\alpha}(\mathfrak{p})=0$.

Case I: $\tau^{\alpha}{}_{q+u_0}(\mathfrak{e})\neq 0$, $1\leqq u_0\leqq n-q$. Then we have

$$\omega^{\alpha}{}_{i}(\mathfrak{g})-x^{\alpha}(\mathfrak{p})\,(\tau^{\alpha}{}_{i}/\tau^{\alpha}{}_{q+u_0})\,(\mathfrak{e})\omega^{\alpha}{}_{q+u_0}(\mathfrak{g})=0, \qquad 1\leqq i\leqq q,$$
$$\omega^{\alpha}{}_{q+u}(\mathfrak{g})-(\tau^{\alpha}{}_{q+u}/\tau^{\alpha}{}_{q+u_0})\,(\mathfrak{e})\omega^{\alpha}{}_{q+u_0}(\mathfrak{g})=0, \qquad 1\leqq u\leqq n-q.$$

This forces $\omega^{\alpha}{}_{q+u_0}(\mathfrak{g})\neq 0$. Consequently, the $n-1$ functions

$$\omega^{\alpha}{}_{i}/\omega^{\alpha}{}_{q+u_0}-x^{\alpha}(\tau^{\alpha}{}_{i}/\tau^{\alpha}{}_{q+u_0}), \qquad 1\leqq i\leqq q,$$
$$\omega^{\alpha}{}_{q+u}/\omega^{\alpha}{}_{q+u_0}-\tau^{\alpha}{}_{q+u}/\tau^{\alpha}{}_{q+u_0}, \qquad 1\leqq u\leqq n-q, u\neq u_0,$$

generate the ideal determined by $\mathcal{B}(\psi)$ in the local ring of $Y(\psi)$ at $(\mathfrak{e}, \mathfrak{g})$. It is clear that $(\mathfrak{e}, \mathfrak{g})$ is a simple point on $\mathcal{B}(\psi)$, and that the projection $\psi_{;1}$ from $\mathcal{B}(\psi)$ onto $\mathfrak{B}(E)$ bi-regularly maps some open neighborhood of $(\mathfrak{e}, \mathfrak{g})$ on $\mathcal{B}(\psi)$ onto an open neighborhood of $\mathfrak{e}$ on $\mathfrak{B}(E)$.

Case II: $\tau^{\alpha}{}_{q+u}(\mathfrak{e}) = 0$ for all $1 \leqq u \leqq n-q$; hence $\tau^{\alpha}{}_{i_0}(\mathfrak{e}) \neq 0$ for some i_0, $1 \leqq i_0 \leqq q$. Then we have

$$\omega^{\alpha}{}_{i}(\mathfrak{g}) - (\tau^{\alpha}{}_{i}/\tau^{\alpha}{}_{i_0})(\mathfrak{e})\,\omega^{\alpha}{}_{i_0}(\mathfrak{g}) = 0, \qquad 1 \leqq i \leqq n-q,$$

$$x^{\alpha}(\mathfrak{p})\,\omega^{\alpha}{}_{q+u}(\mathfrak{g}) - (\tau^{\alpha}{}_{q+u}/\tau^{\alpha}{}_{i_0})(\mathfrak{e})\,\omega^{\alpha}{}_{i_0}(\mathfrak{g}) = 0, \qquad 1 \leqq u \leqq q,$$

$$(\tau^{\alpha}{}_{q+u_1}/\tau^{\alpha}{}_{i_0})(\mathfrak{e})\,\omega^{\alpha}{}_{q+u_2}(\mathfrak{g}) - (\tau^{\alpha}{}_{q+u_2}/\tau^{\alpha}{}_{i_0})(\mathfrak{e})\,\omega^{\alpha}{}_{q+u_1}(\mathfrak{g}) = 0,$$
$$1 \leqq u_1, u_2 \leqq n-q.$$

This forces at least one of the following to be not equal to zero:

$$\omega^{\alpha}{}_{i_0}(\mathfrak{g}), \omega^{\alpha}{}_{q+1}(\mathfrak{g}), \cdots, \omega^{\alpha}{}_{n}(\mathfrak{g}).$$

Assume first that $\omega^{\alpha}{}_{i_0}(\mathfrak{g}) \neq 0$; then the $n-1$ functions

$$\omega^{\alpha}{}_{i}/\omega^{\alpha}{}_{i_0} - \tau^{\alpha}{}_{i}/\tau^{\alpha}{}_{i_0}, \qquad 1 \leqq i \leqq q, i \neq i_0,$$

$$\tau^{\alpha}{}_{q+u}/\tau^{\alpha}{}_{q+u_0} - x^{\alpha}(\omega^{\alpha}{}_{q+u}/\omega^{\alpha}{}_{i_0}), \qquad 1 \leqq u \leqq n-q,$$

generate the ideal determined by $\mathcal{B}(\psi)$ in the local ring of $Y(\psi)$ at $(\mathfrak{e}, \mathfrak{g})$. Next assume that $\omega^{\alpha}{}_{q+u_0}(\mathfrak{g}) \neq 0$ for some u_0, $1 \leqq u_0 \leqq n-q$; then the $n-1$ functions

$$\omega^{\alpha}{}_{i}/\omega^{\alpha}{}_{q+u_0} - (\tau^{\alpha}{}_{i}/\tau^{\alpha}{}_{i_0})\,\omega^{\alpha}{}_{i_0}/\omega^{\alpha}{}_{q+u_0}, \qquad 1 \leqq i \leqq q, i \neq i_0,$$

$$\tau^{\alpha}{}_{q+u}/\tau^{\alpha}{}_{i_0} - (\tau^{\alpha}{}_{q+u_0}/\tau^{\alpha}{}_{i_0})\,\omega^{\alpha}{}_{q+u}/\omega^{\alpha}{}_{q+u_0}, \qquad 1 \leqq u \leqq n-q, u \neq u_0,$$

$$x^{\alpha} - (\tau^{\alpha}{}_{q+u_0}/\tau_{i_0})\,\omega^{\alpha}{}_{i_0}/\omega^{\alpha}{}_{q+u_0}$$

generate the ideal determined by $\mathcal{B}(\psi)$ in the local ring of $Y(\psi)$ at $(\mathfrak{e}, \mathfrak{g})$. In both subcases, it follows immediately that $(\mathfrak{e}, \mathfrak{g})$ is a simple point on $\mathcal{B}(\psi)$. We have by inspection that the open set $\psi_{;1}{}^{-1}(U_{\alpha, i_0})$ is obtained by monoidal transformation of U_{α, i_0} centered on the non-singular subvariety which determines the ideal generated by the $n-q+1$ functions

$$x^{\alpha}$$

$$\tau^{\alpha}{}_{q+u}/\tau^{\alpha}{}_{i_0}, \qquad 1 \leqq u \leqq n-q.$$

in the local ring of each point on U_{α, i_0}.

We have proved that $\mathcal{B}(\psi)$ is a non-singular variety, and that the projection $\psi_{;1}$ is an anti-monoidal transformation whose center is a non-singular

subvariety of dimension $r+q-2=(r-1)+(q-1)$ on $\mathcal{B}(E)$. Let us denote this subvariety, temporarily, by W. We shall exhibit a specific biregular mapping of the dual projective bundle $\mathcal{B}(Q)$ of Q onto W. First let us observe that a point $\mathfrak{e}$ on $U_\alpha \times P_\alpha$ belongs to $W \cap (U_\alpha \times P_\alpha)$ if and only if:

(a) $\mathfrak{p}=\pi_E(\mathfrak{e})$ is a point on V, so that $x^\alpha(\mathfrak{p})=0$.

(b) $\tau^\alpha{}_{q+u}(\mathfrak{e})=0, \qquad 1\leqq u\leqq n-q;$

next if $\mathfrak{e}$ lies on $W \cap (U_\alpha \times P_\alpha) \cap (U_\beta \times P_\beta)$, then we must have

$$\tau^\alpha{}_i(\mathfrak{e})=\rho\sum_{h=1}^{q} E^\beta{}_h{}^\alpha{}_i(\mathfrak{p})\tau^\beta{}_h(\mathfrak{e}), \qquad 1\leqq i\leqq q,$$

since $\tau^\beta{}_{q+u}(\mathfrak{e})=0$ for all $1\leqq u\leqq n-q$. This proves that the restriction of π_E to W equips W with the structure of a projective fiber bundle whose base space is V. With reference to the sheaf Q, we had the transition laws

$$l^\alpha{}_i=\sum_{h=1}^{q} E'^\beta{}_h{}^\alpha{}_i l^\beta{}_h, \qquad 1\leqq i\leqq q,$$

where $E'^\beta{}_h{}^\alpha{}_i$ is the induced function of $E^\beta{}_h{}^\alpha{}_i$ on the subvariety V; it follows by inspection that we can identify the bundle $\mathcal{B}(Q)$ with W according to the rule that the induced homogeneous coordinates $\tau^\alpha{}_1,\cdots,\tau^\alpha{}_q$ on $W\cap(U_\alpha\times P_\alpha)$ are paired with the sections $l^\alpha{}_1,\cdots,l^\alpha{}_q$ over U_α with reference to $\mathcal{B}(Q)$. The restriction of π_E to $\mathcal{B}(Q)$ is equal to π_Q; the induced sheaf of $B(E)$ on the subvariety $\mathcal{B}(Q)$ is equal to $B(Q)$.

Let $\mathfrak{N}_\psi$ denote the anti-center of $\psi_{;1}$; $\mathfrak{N}_\psi$ is a non-singular subvariety of dimension $r+n-2$ on $\mathcal{C}(\psi)$. From § 16, there is the locally free sheaf $S(\psi)$ of dimension one defined on $\mathcal{C}(\psi)$ and with the property

$$\psi_{;2}B(G)\otimes S(\psi)=\psi_{;1}B(E);$$

in the present situation, we obtain by an easy calculation that

$$S(\psi)=\mathcal{L}(-\mathfrak{N}_\psi),$$

recalling that $\mathcal{L}(-\mathfrak{N}_\psi)$ is the sheaf of germs of rational functions on $\mathcal{C}(\psi)$ which are multiples of the divisor $-\mathfrak{N}_\psi$. Thus the basic class $\Theta(S(\psi))$ is the divisor class of $\mathfrak{N}_\psi$, and we have the important formula

$$\psi_{;2}{}^*(\Theta(G))+\Theta(S(\psi))=\psi_{;1}{}^*(\Theta(E));$$

$\psi_{;1}{}^*(\Theta(E))$, resp. $\psi_{;2}{}^*(\Theta(G))$, is the reciprocal image of the divisor class $\Theta(E)$, resp. $\Theta(G)$, with respect to $\psi_{;1}$, resp. $\psi_{;2}$.

Let $U_{\alpha;i,p}$ $(\alpha\in J,\ 1\leqq i,p\leqq n)$ denote the open set on $\mathcal{E}(\psi)$ consisting of all points $(\mathfrak{e},\mathfrak{g})$ on $\mathcal{E}(\psi)\cap(\Sigma_\psi)^{-1}(U_\alpha)$ which satisfy $\tau^\alpha{}_i(\mathfrak{e})\neq 0$, $\omega^\alpha{}_p(\mathfrak{g})\neq 0$. If $U_\alpha\cap V$ is empty, then $\mathfrak{N}_\psi\cap U_{\alpha;i,p}$ is empty. Assume that $U_\alpha\cap V$ is non-empty. If $i>q$, then $\mathfrak{N}_\psi\cap U_{\alpha;i,p}$ is empty. If $i\leqq q$ and $p>q$, then the function

$$\tau^\alpha{}_p/\tau^\alpha{}_i$$

generates the ideal determined by $\mathfrak{N}_\psi$ in the local ring of $\mathcal{E}(\psi)$ at any point on $U_{\alpha;i,p}$. If $i\leqq q$ and $p\leqq q$, then the function

$$x^\alpha$$

generates the ideal determined by $\mathfrak{N}_\psi$ in the local ring of $\mathcal{E}(\psi)$ at any point on $U_{\alpha;i,p}$.

The projection $\psi_{;2}$ is anti-monoidal transformation from $\mathcal{E}(\psi)$ onto $\mathcal{B}(G)$ with a non-singular subvariety on $\mathcal{B}(G)$ for center. In fact, for a point $(\mathfrak{e},\mathfrak{g})$ on $\mathcal{E}(\psi)\cap(\Sigma_\psi)^{-1}(U_\alpha)$, we must have

$$\rho_1 x^\alpha(\mathfrak{p})\omega^\alpha{}_{q+u}(\mathfrak{g})=\rho_2\tau^\alpha{}_{q+u}(\mathfrak{e}) \qquad 1\leqq u\leqq n-q;$$

$$\rho_1\omega^\alpha{}_i(\mathfrak{g})=\rho_2\tau^\alpha{}_i(\mathfrak{e}), \qquad 1\leqq i\leqq q,$$

the discussion in cases I and II is simply repeated but now with $\omega^\alpha{}_1,\cdots,\omega^\alpha{}_q$ playing the former roles of $\tau^\alpha{}_{q+1},\cdots,\tau^\alpha{}_n$. The center of $\psi_{;2}$ is a subvariety Z of dimension $r+n-q-2=(r-1)+(n-q-1)$ on $\mathcal{B}(G)$; the $q+1$ functions

$$\omega^\alpha{}_i/\omega^\alpha{}_{q+u}, \qquad 1\leqq i\leqq q,$$

$$x^\alpha$$

generate the ideal determined by Z in the local ring of $\mathcal{B}(G)$ at each point of $U'_{\alpha,q+u}$; $Z\cap U'_{\alpha,i}$ is empty if $1\leqq i\leqq q$. The restriction of π_G to Z equips Z with the structure of a projective fiber bundle whose base space is V; as such Z is the dual projective bundle of the locally free sheaf $M(\psi)$ defined on V, and we set $Z=\mathcal{B}(M(\psi))$. $\pi_G{}^{-1}(V)$, the portion of $\mathcal{B}(G)$ over V, is a non-singular subvariety of dimension $r+n-2$ on $\mathcal{B}(G)$; the restriction of π_G to that subvariety equips it with the structure of the dual projective bundle $\mathcal{B}(G')$ of the induced sheaf G' of G on the subvariety V. We observe that $\mathcal{B}(M(\psi))$ is a subvariety on $\mathcal{B}(G')$.

Let $\mathfrak{M}_\psi$ denote the anti-center of $\psi_{;2}$. If $U_\alpha\cap V$ is empty, then $\mathfrak{M}_\psi\cap U_{\alpha;i,p}$ is empty. Assume that $U_\alpha\cap V$ is not empty. If $p\leqq q$, then $\mathfrak{M}_\psi\cap U_{\alpha;i,p}$ is empty. If $p>q$ and $i\leqq q$, then the function

$$\omega^\alpha{}_i/\omega^\alpha{}_p$$

generates the ideal determined by $\mathcal{M}_\psi$ in the local ring of $\mathcal{B}(\psi)$ at any point on $U_{\alpha;i,p}$; if $p > q$ and $i > q$, then the function

$$x^\alpha$$

generates the ideal determined by $\mathcal{M}_\psi$ in the local ring of $\mathcal{B}(\psi)$ at any point on $U_{\alpha;i,p}$. The divisor $\psi_{;2}^*(\mathcal{B}(G'))$, which is the reciprocal image of the divisor $\mathcal{B}(G')$ on $\mathcal{B}(G)$ with respect to $\psi_{;2}$ and also the total transform of $\mathcal{B}(G')$ with respect to the inverse of $\psi_{;2}$, is the divisor $\mathcal{M}_\psi + \mathcal{N}_\psi$; that is to say,

$$\psi_{;2}^*(\mathcal{B}(G')) = \mathcal{M}_\psi + \mathcal{N}_\psi.$$

The intersection cycle $\mathcal{M}_\psi \circ \mathcal{N}_\psi$ is a non-singular subvariety of dimension $r + n - 2$ on $\mathcal{B}(\psi)$; the restriction of $\psi_{;2}$ to $\mathcal{N}_\psi$ is an anti-monoidal transformation of $\mathcal{N}_\psi$ onto $\mathcal{B}(G')$ whose anti-center is $\mathcal{M}_\psi \circ \mathcal{N}_\psi$ and with center $\mathcal{B}(M(\psi))$ as subvariety on $\mathcal{B}(G')$. The restriction of $\psi_{;1}$ to $\mathcal{M}_\psi$ is an anti-monoidal transformation from $\mathcal{M}_\psi$ onto the non-singular subvariety $\mathcal{B}(E')$ on $\mathcal{B}(E)$, where $\mathcal{B}(E')$ is the dual projective bundle of the induced sheaf E' of E on the subvariety V on X, whose anti-center is $\mathcal{M}_\psi \circ \mathcal{N}_\psi$ and with center $\mathcal{B}(Q)$ as subvariety on $\mathcal{B}(E')$. $\psi_{;1}^*(\mathcal{B}(E'))$, the reciprocal image of the divisor $\mathcal{B}(E')$ on $\mathcal{B}(E)$, is the divisor $\mathcal{M}_\psi + \mathcal{N}_\psi$; consequently, we have

$$\psi_{;2}^*(\mathcal{B}(G')) = \mathcal{M}_\psi + \mathcal{N}_\psi = \psi_{;1}^*(\mathcal{B}(E')).$$

§ 20. We shall prove that the dual projective bundle $\mathcal{B}(E)$ admits a projective model. Let $\mathcal{O}_X{}^N$ denote the direct sum $\mathcal{O}_X + \cdots + \mathcal{O}_X$ taken N times. It is obvious that $\mathcal{B}(\mathcal{O}_X{}^N)$ is the product variety of X and a projective space of dimension $N - 1$; hence, $\mathcal{B}(\mathcal{O}_X{}^N)$ admits a projective model since we have supposed that X admits a projective model. With respect to a specific projective imbedding of X we denote by D_h the locally free sheaf of dimension one defined on X such that $\Theta(D_h)$ is the divisor class of the linear system of hypersurface sections of degree h on X. Now we have

$$\mathcal{B}(\mathcal{O}_X{}^N \otimes D_h) = \mathcal{B}(\mathcal{O}_X{}^N),$$

and it is an elementary fact (the construction of the projective model of the product of two projective models) that for any $h > 0$, the linear system of positive divisors from the divisor class $\Theta(\mathcal{O}_X{}^N \otimes D_h)$ serves as a system of hyperplane sections for a projective model for $\mathcal{B}(\mathcal{O}_X{}^N)$.

On the other hand, we have, from one of Serre's fundamental theorems, that if we are given a sheaf E, then, for all sufficiently large positive integers

h_0, we can choose $\mathcal{O}_X{}^N$ and a homomorphism ψ of $\mathcal{O}_X{}^N$ onto $E \otimes D_{h_0}$. Assuming that E is a locally free sheaf and applying the results of § 17, we have that $\mathcal{B}(\psi)$ is a bi-regular mapping of $\mathcal{B}(E)$—which is the same as $\mathcal{B}(E \otimes D_{h_0})$—onto a subvariety on $\mathcal{B}(\mathcal{O}_X{}^N)$. This proves that $\mathcal{B}(E)$ admits a projective model and that the linear system of positive divisors from $\Theta(E \otimes D_{h_0+1})$ serves a system of hyperplane sections for a projective model of $\mathcal{B}(E)$.

IV. The Unicity of the $\mathcal{A}$-genus.

§ 21. By an arithmetic functional, we shall mean a mapping $\mathcal{A}$ which assigns a rational number $\mathcal{A}(X)$ to every non-singular projective model X and satisfies the following axioms:

Axiom I: (Normalization) $\mathcal{A}(P) = 1$ for any projective space; $\mathcal{A}(\emptyset) = 0$, where $\emptyset$ is the empty variety.

Axiom II: (Modular Law) X is a non-singular projective model of dimension r; A, A' are non-singular subvarieties of dimension $r-1$ on X; the intersection cycle $A \circ A'$ is proper and

$$A \circ A' = \sum_{i=1}^{s} V_i,$$

where V_i is a non-singular subvariety of dimension $r-2$ on X for all $1 \leqq i \leqq s$, and $V_i \cap V_j$ is empty if $i \neq j$, $1 \leqq i, j \leqq s$; finally, there is a non-singular subvariety A_1 of dimension $r-1$ on X such that the divisor A_1 is linearly equivalent to the divisor $A + A'$. In these circumstances, we require that

$$\mathcal{A}(A_1) = \mathcal{A}(A) + \mathcal{A}(A') - \sum_{i=1}^{s} \mathcal{A}(V_i).$$

Axiom III: (Fiber Law) Y, X are non-singular projective models; $\Phi: Y \to X$ is a rational transformation from Y onto X which satisfies either of the following conditions:

(a) Φ equips Y with the structure of the dual projective bundle of some locally free sheaf defined on X;

(b) Y is obtained by monoidal transformation of X centered on a non-singular subvariety on X with Φ the anti-monoidal transformation. Then we require that

$$\mathcal{A}(Y) = \mathcal{A}(X).$$

In this chapter, we assume the existence of an arithmetic functional $\mathfrak{A}$; $\mathfrak{A}(X)$ is called the $\mathfrak{A}$-genus of the variety X. The main issue will be to prove that $\mathfrak{A}$ is unique.

§ 22. Our aim is to define the "virtual" $\mathfrak{A}$-genus of an arbitrary divisor class on a non-singular projective model X. To this end, we must repeat for the $\mathfrak{A}$-genus the familiar arguments used to define the virtual arithmetic genus.

We note first that $\mathfrak{A}(X)$ is a bi-regular invariant of the non-singular projective model X; this is the weak form of the Fiber Law (Axiom III) which corresponds to the case where Φ is a bi-regular mapping.

Next, if A, A_1 are non-singular subvarieties of dimension $r-1$ on X ($\dim. X=r$) and if A, A_1 are linearly eqivalent as divisors on X, then, as follows from the Modular Law (Axiom II) by taking A' equal to the empty variety and using Axiom I,

$$\mathfrak{A}(A_1)=\mathfrak{A}(A). \tag{1}$$

Let x be a divisor class on X, and assume that there exists a non-singular subvariety A of dimension $r-1$ which, as divisor, belongs to x. In this situation, we define $\mathfrak{A}(x)$, the $\mathfrak{A}$-genus of the divisor class x, according to

$$\mathfrak{A}(x)=\mathfrak{A}(A);$$

$\mathfrak{A}(x)$ depends solely upon x, as follows from (1). (If $\dim. X=1$, and if x contains a positive divisor A of type $\mathfrak{p}_1+\cdots+\mathfrak{p}_s$ with $\mathfrak{p}_1,\cdots,\mathfrak{p}_s$ different points of X, then we define

$$\mathfrak{A}(x)=\mathfrak{A}(A)=s;$$

this definition is consistent with Axiom I and the Modular Law.)

Now assume that x is sufficiently ample (i.e., the positive divisors of x serve as a system of hyperplane sections for some projective imbedding of X). Then $\mathfrak{A}(x)$ is defined as above. We define $\mathfrak{A}(x^k)$ according to

$$\mathfrak{A}(x^k)=\mathfrak{A}(A_1\circ\cdots\circ A_k),$$

where $A_1\circ\cdots\circ A_k$ is the intersection cycle formed by k-general members of x; this cycle is a non-singular subvariety of co-dimension k on X (with the obvious modification if $k=f=\dim. X$); $\mathfrak{A}(x^k)$ depends solely upon x, as follows by repeating the argument used to obtain (1); furthermore, if $k>r$, then $\mathfrak{A}(x^k)=0$, as follows from Axiom I.

Let W be a non-singular subvariety on X, and let $\{x\}_W$ denote the trace

of x on W. Then $\{x\}_W$ is a sufficiently ample divisor class on W; hence, $\mathcal{A}((\{x\}_W)^k)$ is defined for all k and we have

$$\mathcal{A}((\{x\}_W)^k) = \mathcal{A}(A_1 \circ \cdots \circ A_k \circ W).$$

Let $x, y, z, \cdots$ be sufficiently ample divisor classes on X. Then $x + y$, $x + z, y + z, \cdots$ are sufficiently ample divisor classes on X. We consider $\mathcal{A}((\{x\}_B)^k)$, where B is a sufficiently general member of y; it depends solely upon x and y and we set

$$\mathcal{A}((\{x\}_y)) = \mathcal{A}((\{x\}_B)).$$

Similarly, we set

$$\mathcal{A}((\{x\}_{y \circ z})^k) = \mathcal{A}((\{x\}_{B \circ C})^k),$$

where B, C are general members of y and z respectively, and we have

$$\mathcal{A}((\{x\}_{y \circ z})^k) = \mathcal{A}(A_1 \circ \cdots \circ A_k \circ B \circ C).$$

Let D be a non-singular member of the divisor class $y + z$. Then, as a consequence of the Modular Law, we have

$$\mathcal{A}((\{x\}_D)^k) = \mathcal{A}((\{x\}_B)^k) + \mathcal{A}((\{x\}_C)^k) - \mathcal{A}((\{x\}_{B \circ C})^k);$$

but we can rewrite this formula as

$$\mathcal{A}((\{x\}_{y+z})^k) = \mathcal{A}((\{x\}_y)^k) + \mathcal{A}((\{x\}_z)^k) - \mathcal{A}((\{x\}_{y \circ z})^k). \tag{2}$$

Define the quantity $\mathcal{K}(x)$ according to

$$\mathcal{K}(x) = \mathcal{A}(X) + \sum_{k=1}^{\infty} \mathcal{A}(x^k),$$

and observe that

$$\mathcal{K}(x) = \mathcal{A}(X) + \mathcal{K}(\{x\}_x). \tag{3}$$

The quantity $\mathcal{K}(\{x\}_W)$ is well defined for any non-singular subvariety W and

$$\mathcal{K}(\{x\}_W) = \mathcal{A}(W) + \sum_{k=1}^{\infty} \mathcal{A}(\{x\}_W{}^k).$$

In particular, $\mathcal{K}(\{x\}_B)$ is defined for any general member B of y, and we set

$$\mathcal{K}(\{x\}_y) = \mathcal{K}(\{x\}_B),$$

observing that $\mathcal{K}(\{x\}_y)$ depends solely upon x and y. Similarly, $\mathcal{K}(\{x\}_{y \circ z})$ is well defined and

$$\mathcal{K}(\{x\}_{y \circ z}) = \mathcal{K}(\{x\}_{B \circ C}).$$

From (2), we obtain

$$\mathcal{K}(\{x\}_{y+z}) = \mathcal{K}(\{x\}_y) + \mathcal{K}(\{x\}_z) - \mathcal{K}(\{x\}_{y \circ z}). \tag{4}$$

PROPOSITION 1.

$$\mathcal{K}(x+y)=\mathcal{K}(x)+\mathcal{K}(\{x+y\}_y). \tag{5}$$

Proof. The proof is by induction on the dimension r of the ambient variety X. The proposition is evident if the ambient variety is of dimension one; we asume that it is true whenever the ambient variety is of dimension less than r. From (3), we have

$$\mathcal{K}(x+y)=\mathfrak{a}(X)+\mathcal{K}(\{x+y\}_{x+y});$$

from (4), we have

$$\mathcal{K}(\{x+y\}_{x+y})=\mathcal{K}(\{x+y\}_x)+\mathcal{K}(\{x+y\}_y)-\mathcal{K}(\{x+y\}_{x\circ y});$$

the inductive assumption gives

$$\mathcal{K}(\{x\}_x=\mathcal{K}(\{x+y\}_x)-\mathcal{K}(\{x+y\}_{x\circ y}),$$

where the ambient variety is a general member of x; this gives

$$\mathcal{K}(\{x+y\}_{x+y})=\mathcal{K}(\{x\}_x)+\mathcal{K}(\{x+y\}_y),$$

and the proposition is proved by adding $\mathfrak{a}(X)$ to both sides.

PROPOSITION 2.

$$\mathcal{K}(\{y+z\}_{x+z})-\mathcal{K}(\{y+z\}_{y+z})=\mathcal{K}(\{y\}_x)-\mathcal{K}(\{y\}_y). \tag{6}$$

Proof. Applying (4), we have

$$\mathcal{K}(\{y+z\}_{x+z})=\mathcal{K}(\{y+z\}_x)+\mathcal{K}(\{y+z\}_z)-\mathcal{K}(\{y+z\}_{x\circ z});$$

from Proposition 1, we have

$$\mathcal{K}(\{y\}_x)=\mathcal{K}(\{y+z\}_x)-\mathcal{K}(\{y+z\}_{x\circ z}),$$

which proves that

$$\mathcal{K}(\{y+z\}_{x+z})=\mathcal{K}(\{y\}_x)+\mathcal{K}(\{y+z\}_z); \tag{7}$$

similarly, we have

$$\mathcal{K}(\{y+z\}_{y+z})=\mathcal{K}(\{y\}_y)+\mathcal{K}(\{y+z\}_z); \tag{8}$$

hence, (6) follows by substracting (8) from (7).

Let ϑ be an arbitrary divisor class on X. Then it is possible to choose sufficiently ample divisor classes x, y on X with the property $\vartheta=x-y$. We define $\mathfrak{a}(\vartheta)$, the virtual $\mathfrak{a}$-genus ϑ, according to

$$\mathfrak{a}(\vartheta)=\mathfrak{a}(x-y)=\mathcal{K}(\{y\}_x)-\mathcal{K}(\{y\}_y). \tag{9}$$

On the basis of Proposition 2, it follows that $\mathfrak{A}(\vartheta)$ depends solely upon ϑ. The explicit formula is

$$(10)\quad \mathfrak{A}(\vartheta)=\mathfrak{A}(A)+\sum_{k=1}^{r-1}\mathfrak{A}(B_1\circ\cdots\circ B_k\circ A) -\mathfrak{A}(B)-\sum_{k=1}^{r-1}\mathfrak{A}(B_1\circ\cdots\circ B_k\circ B),$$

where A (resp. $B, B_1,\cdots, B_{r-1}$) are general members of x (resp. y). If ϑ contains a non-singular member U, then

$$(11)\qquad \mathfrak{A}(\vartheta)=\mathfrak{A}(U);$$

for A, $B+U$ are linearly equivalent divisors on X and from the Modular Law, we have that

$$\mathfrak{A}(A)=\mathfrak{A}(B)+\mathfrak{A}(U)-\mathfrak{A}(B\circ U),$$

$$\mathfrak{A}(B_1\circ\cdots\circ B_k\circ A)=\mathfrak{A}(B_1\circ\cdots\circ B_k\circ B)+\mathfrak{A}(B_1\circ\cdots\circ B_k\circ U) -\mathfrak{A}(B_1\circ\cdots\circ B_k\circ B\circ U).$$

(11) follows by summation of these last equations followed by subtraction of $\sum_{k=1}^{r-1}\mathfrak{A}(B_1\circ\cdots\circ B_k\circ B)$.

For an arbitrary divisor class ϑ, we define $\mathcal{K}(\vartheta)$ according to

$$(12)\qquad \mathcal{K}(\vartheta)=\mathcal{K}(x-y)=\mathcal{K}(x)-\mathcal{K}(\{x\}_y),$$

where $\vartheta=x-y$, x, y sufficiently ample. (If ϑ is sufficiently ample, then this agrees with the previous definition as follows from Proposition 1.) From the equation $\mathcal{K}(x)=\mathfrak{A}(X)+\mathcal{K}(\{x\}_x)$ and the definition of $\mathfrak{A}(-\vartheta)$ $=K(y-x)$, it is evident that

$$(13)\qquad \mathcal{K}(\vartheta)=\mathfrak{A}(X)-\mathfrak{A}(-\vartheta).$$

THEOREM 1. *Let ϑ, ϑ_1 be arbitrary divisor classes on X with the property that $\vartheta-\vartheta_1$ contains a non-singular member T. Then*

$$(14)\qquad \mathcal{K}(\vartheta)=\mathcal{K}(\vartheta_1)+\mathcal{K}(\{\vartheta\}_T),$$

where $\{\vartheta\}_T$ denotes the trace of ϑ on T, and

$$(15)\qquad \mathfrak{A}(\vartheta)=\mathfrak{A}(\vartheta_1)+\mathfrak{A}(T)-\mathfrak{A}(\{\vartheta_1\}_T).$$

Proof. It is possible to choose sufficiently ample divisor classes x, y, y_1 such that $\vartheta=x-y$; $\vartheta_1=x-y_1$; thus T is a member of y_1-y. Now

$$\mathcal{K}(\vartheta_1)=\mathcal{K}(x-y_1)=\mathcal{K}(x)-\mathcal{K}(\{x\}_{y_1}),$$

and from the Modular Law,

$$\mathscr{K}(\{x\}_{y_1}) = \mathscr{K}(\{x\}_y) + \mathscr{K}(\{x\}_T) - \mathscr{K}(\{x\}_{y\circ T})$$

(where $\mathscr{K}(\{x\}_{y\circ T}) = \mathscr{K}(\{x\}_{B\circ T})$ with B a general member of y), which yields

$$\mathscr{K}(\vartheta_1) = \mathscr{K}(x) - \mathscr{K}(\{x\}_y) - \mathscr{K}(\{x\}_T) + \mathscr{K}(\{x\}_{y\circ T}). \tag{16}$$

But

$$\mathscr{K}(\vartheta) = \mathscr{K}(x) - \mathscr{K}(\{x\}_y)$$

and

$$\mathscr{K}(\{\vartheta\}_T) = \mathscr{K}(\{x\}_T) - \mathscr{K}(\{x\}_{y\circ T})$$

from the definition of $\mathscr{K}(\vartheta)$, $\mathscr{K}\{\vartheta\}_T)$; hence (14) follows from (16). We obtain immediately from (14) that

$$\mathscr{K}(-\vartheta_1) = \mathscr{K}(-\vartheta) + \mathscr{K}(-\{\vartheta_1\}_T). \tag{17}$$

But

$$\begin{aligned} \mathscr{K}(-\vartheta_1) &= \mathfrak{a}(X) - \mathfrak{a}(\vartheta_1), \\ \mathscr{K}(-\vartheta) &= \mathfrak{a}(X) - \mathfrak{a}(\vartheta), \\ \mathscr{K}(\{-\vartheta_1\}_T) &= \mathfrak{a}(T) - \mathfrak{a}(\{\vartheta_1\}_T); \end{aligned}$$

hence (15) follows from (17).

§ 23. X, Y are non-singular projective models and Φ is a regular mapping from Y into X—eventually we shall assume that Φ satisfies one of the conditions required by the Fiber Law. Given a divisor class ϑ on X, then there is a divisor class $\Phi^*\vartheta$ on Y which is the reciprocal image of ϑ with respect to Φ. If D is a locally free sheaf of dimension one defined on X such that $\vartheta = \Theta(D)$, the basic class of D, then $\Phi^*\vartheta$ is the basic class of ΦD, the reciprocal image of D with respect to Φ.

Specifically, if there exists a posittive divisor A which belongs to ϑ and with the property that no component of A contains the image of Y in X—and this property will be automatically true if Φ satisfies one of the conditions of the Fiber Law—then there is the reciprocal image divisor Φ^*A on Y which is defined as follows: Let $f = 0$ be a local equation for A on an open subset U of X; then $\Phi^{-1}f = 0$ is a local equation for Φ^*A on $\Phi^{-1}(U)$, where $\Phi^{-1}f$ is the image of f under the natural homomorphism from $\Gamma(\mathcal{O}_U, U)$ into $\Gamma(\mathcal{O}_{\Phi^{-1}(U)}, \Phi^{-1}(U))$. The divisor Φ^*A belongs to the class $\Phi^*\vartheta$. Consequently, if x is a sufficiently ample divisor class on X, then for a general positive member A of x, we have that Φ^*A is an irreducible non-singular subvariety on X (with the usual modification for dim. $X = 1$).

Now assume that Φ satisfies the condition (a) in the Fiber Law, so that Φ equips Y with the structure of the dual projective bundle of some locally free sheaf S defined on X. Let x be a sufficiently ample divisor class on X and let A be a general member of X. Then the restriction of Φ to Φ^*A equips Φ^*A with the structure of the dual projective bundle of the induced sheaf of S on the subvariety A, and from the Fiber Law, we have $\mathfrak{a}(\Phi^*A) = \mathfrak{a}(A)$, which proves that

$$\mathfrak{a}(\Phi^*x) = \mathfrak{a}(x).$$

Let ϑ be an arbitrary divisor class on X and choose sufficiently ample divisor classes x, y with $\vartheta = x - y$; A, B are general members of x, y respectively. Applying Theorem 1 on the variety Y, we have

$$\mathfrak{a}(\Phi^*x) = \mathfrak{a}(\Phi^*\vartheta) + \mathfrak{a}(\Phi^*B) - \mathfrak{a}(\{\Phi^*\vartheta\}_{\Phi^*B})$$

since Φ^*B is a non-singular member of $\Phi^*\vartheta - \Phi^*x$, and on X, we have

$$\mathfrak{a}(x) = \mathfrak{a}(\vartheta) + \mathfrak{a}(B) - \mathfrak{a}(\{\vartheta\}_B).$$

Then we obtain, by induction on the dimension of the ambient variety X, that

$$(1) \qquad \mathfrak{a}(\Phi^*\vartheta) = \mathfrak{a}(\vartheta);$$

for we have $\mathfrak{a}(x) = \mathfrak{a}(\Phi^*x)$, $\mathfrak{a}(B) = \mathfrak{a}(\Phi^*B)$ and, since $\dim. B$ is less than $\dim. X$, the inductive assumption gives $\mathfrak{a}(\{\vartheta\}_B) = \mathfrak{a}(\{\Phi^*\vartheta\}_{\Phi^*B})$. We have, as an immediate consequence of (1), that

$$(2) \qquad \mathcal{K}(\Phi^*\vartheta) = \mathcal{K}(\vartheta).$$

Now assume that Φ satisfies the condition (b) of the Fiber Law, so that Y is obtained by monoidal transformation of X centered on a non-singular subvariety V on X and Φ is the anti-monoidal transformation. If A is a general member of a sufficiently ample divisor class x on X, then Φ^*A is a non-singular subvariety on Y and Φ^*A is the variety obtained by monoidal transformation of A centered on the intersection cycle $A \circ V$; the cycle $A \circ V$ is a non-singular subvariety of dimension $n-1$ on X if $\dim. V = n$, for a general member A of x; the restriction of Φ to Φ^*A is the anti-monoidal transformation. (If $n = 1$, then $A \circ V = \mathfrak{p}_1 + \cdots + \mathfrak{p}_s$ with $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ different points on A and Φ^*A is obtained by successive monoidal transformations of A centered at the points $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$.) The arguments of the previous paragraph can be repeated and we again have that

$$\mathcal{A}(\Phi^*\vartheta) = \mathcal{A}(\vartheta), \tag{1}$$

$$\mathcal{K}(\Phi^*\vartheta) = \mathcal{K}(\vartheta), \tag{2}$$

where Φ satisfies condition (b) of the Fiber Law.

THEOREM 2. *Let $\Phi: Y \to X$ satisfy one of the conditions of the Fiber Law. Then for any divisor class ϑ on X, we have*

$$\mathcal{A}(\Phi^*\vartheta) = \mathcal{A}(\vartheta),$$

$$\mathcal{K}(\Phi^*\vartheta) = \mathcal{K}(\vartheta).$$

The following proposition is essentially a corollary to Theorem 2, and it is used extensively in the next §.

PROPOSITION 3. *Let E be a locally free sheaf defined on X, and let $\Phi: Y \to X$ be as in the Fiber Law. Then*

$$\mathcal{A}(\Theta(\Phi E)) = \mathcal{A}(\Theta(E)), \tag{3}$$

$$\mathcal{K}(\Theta(\Phi E)) = \mathcal{K}(\Theta(E)). \tag{4}$$

Proof. We recall from § 8 of Chap. I that $\mathcal{B}(\Phi E)$ is the induced bundle of $\mathcal{B}(E)$ from the mapping $\Phi: Y \to X$ of the base spaces, $B(\Phi E)$ is the reciprocal image of $B(E)$ with respect to the fiber preserving map from $\mathcal{B}(\Phi E)$ to $\mathcal{B}(E)$ over $\Phi: Y \to X$, and $\Theta(\Phi E)$ is the reciprocal image of $\Theta(E)$ with respect to the fiber preserving map. But, by inspection, it is evident that the fiber preserving map from $\mathcal{B}(\Phi E)$ onto $\mathcal{B}(E)$ satisfies one of the conditions of the Fiber Law since Φ has this property, and our conclusions follow from Theorem 2.

§ 24. Given a locally free sheaf E defined on a non-singular projective model X, we define $\mathcal{K}(E)$, the $\mathcal{K}$-characteristic of the sheaf E, according to

$$\mathcal{K}(E) = \mathcal{K}(\Theta(E)) = \mathcal{A}(\mathcal{B}(E)) - \mathcal{A}(-\Theta(E)). \tag{1}$$

For the sheaf $\mathcal{O}_X$ of local rings on X, we have

$$\mathcal{K}(\mathcal{O}_X) = \mathcal{A}(X) \tag{2}$$

since $\Theta(\mathcal{O}_X)$ is the divisor class zero on X.

We have

$$\mathcal{K}(B(E)) = \mathcal{K}(E) \tag{3}$$

since $\Theta(B(E)) = \Theta(E)$ and $\mathcal{A}(X) = \mathcal{A}(\mathcal{B}(E))$.

PROPOSITION 4. *X, Y are non-singular projective models, $\Phi: Y \to X$ satisfies one of the conditions of the Fiber Law. Then for any locally free sheaf E defined on X, we have*

$$\mathcal{K}(\Phi E) = \mathcal{K}(E). \tag{4}$$

Proof. This is a restatement of Proposition 3 which gave $\mathcal{K}(\Theta(\Phi E)) = \mathcal{K}(\Theta(E))$.

THEOREM 3. *Let*

$$0 \to H \xrightarrow{\theta} G \xrightarrow{\psi} E \to 0 \tag{5}$$

be an exact sequence of locally free sheaves defined on X. Then

$$\mathcal{K}(G) = \mathcal{K}(H) + \mathcal{K}(E).$$

Proof. We refer to the results and notations of § 17, Chap. III where the geometric resolution of (5) is discussed in detail. On the graph $\mathcal{G}(\theta)$, there are the projections $\theta_{;1}$: $\mathcal{G}(\theta) \to \mathcal{B}(G)$ and $\theta_{;2}$: $\mathcal{G}(\theta) \to \mathcal{B}(H)$; $\theta_{;1}$ is an anti-monoidal transformation whose center is the subvariety $\mathcal{B}(E)$ on $\mathcal{B}(G)$ and whose anti-center is $\mathcal{N}_\theta$; $\theta_{;2}$ equips $\mathcal{G}(\theta)$ with the structure of the dual projective bundle of the locally free sheaf $R(\theta)$ defined on $\mathcal{B}(H)$; thus both $\theta_{;1}$ and $\theta_{;2}$ satisfy one of the conditions of the Fiber Law. On $\mathcal{G}(\theta)$, we have

$$\theta_{;1}{}^*\Theta(G) = \theta_{;2}{}^*\Theta(H) + \Theta(S(\theta)) \tag{6}$$

and the non-singular subvariety $\mathcal{N}_\theta$ belongs to the divisor class $\Theta(S(\theta))$. Set $x = \theta_{;1}{}^*\Theta(G)$, $y = \theta_{;2}{}^*\Theta(H)$ and $s = \Theta(S(\theta))$ so that (6) is identical to

$$x = y + s. \tag{6'}$$

We can apply Theorem 1 since $s = x - y$ contains the non-singular member $\mathcal{N}_\theta$ and we have

$$\mathcal{K}(x) = \mathcal{K}(y) + \mathcal{K}(\{x\}_{\mathcal{N}_\theta}); \tag{7}$$

from Theorem 2, we have $\mathcal{K}(x) = \mathcal{K}(\Theta(G))$ and $\mathcal{K}(y) = \mathcal{K}(\Theta(H))$ since both $\theta_{;1}$ and $\theta_{;2}$ satisfy one of the conditions of the Fiber Law; $\{x\}_{\mathcal{N}_\theta}$, the trace of x on the subvariety $\mathcal{N}_\theta$, is equal to the reciprocal image of $\Theta(E)$ with respect to the restriction of $\theta_{;1}$ to $\mathcal{N}_\theta$ and, since this restriction mapping equips $\mathcal{N}_\theta$ with the structure of the dual projective bundle of the sheaf

$N(\mathcal{B}(G), \mathcal{B}(E))$, we can again apply Theorem 2 to obtain that $\mathcal{K}(\{x\}_{\mathcal{N}_0}) = \mathcal{K}(\Theta(E))$. Substituting in (7), we obtain

$$\mathcal{K}(\Theta(G)) = \mathcal{K}(\Theta(H)) + \mathcal{K}(\Theta(E)),$$

which proves the theorem.

THEOREM 4. *Let*

$$0 \to G \xrightarrow{\psi} E \to Q \to 0 \tag{8}$$

be an exact sequence of sheaves defined on X of the type described in § 18, § 19 *of Chap.* III. *Then*

$$\mathcal{K}(E) = \mathcal{K}(G) + \mathcal{K}(Q). \tag{9}$$

Proof. The proof is similar to that of the previous theorem, but we refer now to the results and notations of § 18, § 19 of Chap. III. On the graph $\mathcal{G}(\psi)$, we have

$$\psi_{;1}{}^{*}\Theta(E) = \psi_{;2}{}^{*}\Theta(G) + \Theta(S(\psi));$$

$\psi_{;1}$ (resp. $\psi_{;2}$) is an anti-monoidal transformation from $\mathcal{G}(\psi)$ onto $\mathcal{B}(E)$ resp. $\mathcal{B}(G)$); $\mathcal{N}_{\psi}$ belongs to the divisor class $\Theta(S(\psi))$ and the restriction of $\psi_{;1}$ equips $\mathcal{N}_{\psi}$ with the structure of the dual projective bundle of the sheaf $N(\mathcal{B}(E); \mathcal{B}(Q))$. Set $x = \psi_{;1}{}^{*}\Theta(E)$, $y = \psi_{;2}{}^{*}\Theta(G)$ and $s = \Theta(S(\psi))$. We can apply Theorem 1 since $s = x - y$ contains the non-singular member $\mathcal{N}_{\psi}$ and we have

$$\mathcal{K}(x) = \mathcal{K}(y) + \mathcal{K}(\{x\}_{\mathcal{N}_{\psi}}). \tag{10}$$

The divisor class $\{x\}_{\mathcal{N}_{\psi}}$, which is the trace of x on the subvariety $\mathcal{N}_{\psi}$, is the reciprocal image of the divisor class $\Theta(Q)$ with respect to the bundle projection from $\mathcal{N}_{\psi}$ onto $\mathcal{B}(Q)$. From Theorem 2, we have

$$\mathcal{K}(x) = \mathcal{K}(\Theta(E)),$$
$$\mathcal{K}(y) = \mathcal{K}(\Theta(G)),$$
$$\mathcal{K}(\{x\}_{\mathcal{N}_{\psi}}) = \mathcal{K}(\Theta(Q)),$$

so that (9) follows by substitution in (10).

§ 25. Consider the exact sequence

$$0 \to F^{r-d} \xrightarrow{\psi^{r-d}} \cdots \to F^{s} \xrightarrow{\psi^{s}} F^{s-1} \to \cdots \to F^{0} \xrightarrow{\psi^{0}} Q \to 0 \tag{1}$$

of § 13, Chap. II; $F^{r-d}, \cdots, F^0$ are locally free sheaves defined on X; Q is the extension to X of a locally free sheaf defined on V, which sheaf we continue to denote as Q, where V is a non-singular subvariety of dimension d on X with $\dim. X = r$. The following theorem is of fundamental importance in the proof of the unicity of $\mathfrak{a}$.

THEOREM 5. *For the exact sequence* (1), *we have*

$$\mathcal{K}(Q) = \sum_{l=0}^{r-d} (-1)^l \mathcal{K}(F^l). \tag{2}$$

The remainder of this § is devoted to proof of (2) which depends upon a lemma to be stated here but proved in the next §. X^* is the variety obtained from monoidal transformation of X centered on V; Φ is the anti-monoidal transformation from X^* onto X and V^* is the anti-center. Using the notations of § 13, we have the exact sequences

$$0 \to \operatorname{Im}[\psi_*{}^1] \to F_*{}^0 \to Q_* \to 0, \tag{3}$$

$$0 \to \operatorname{Im}[\psi_*{}^{s+1}] \to \operatorname{Ker}[\psi_*{}^s] \to Q_* \otimes \wedge^s(\delta N) \to 0 \tag{4}$$

for $1 \leqq s \leqq r-d-1$ and

$$0 \to \operatorname{Ker}[\psi_*{}^s] \to F_*{}^s \to \operatorname{Im}[\psi_*{}^s] \to 0 \tag{5}$$

for $1 \leqq s \leqq r-d$. We can apply Theorem 3 to (5) since (5) is an exact sequence of locally free sheaves defined on X^* and we obtain

$$\mathcal{K}(\operatorname{Im}[\psi_*{}^s]) = \mathcal{K}(F_*{}^s) - \mathcal{K}(\operatorname{Ker}[\psi_*{}^s]) \tag{6}$$

for $1 \leqq s \leqq r-d$. We can apply Theorem 4 to the exact sequences (4) and (3) since Q_* (resp. $Q_* \otimes \wedge^s(\delta N)$) is a locally free sheaf defined on the subvariety V^* of co-dimension 1 on X^*; thus we obtain

$$\mathcal{K}(Q_*) = \mathcal{K}(F_*{}^0) - \mathcal{K}(\operatorname{Im}[\psi_*{}^1]) \tag{7}$$

and

$$\mathcal{K}(Q_* \otimes \wedge^s(\delta N)) = \mathcal{K}(\operatorname{Ker}[\psi_*{}^s]) - \mathcal{K}(\operatorname{Im}[\psi_*{}^{s+1}]) \tag{8}$$

for $1 \leqq s \leqq r-d-1$. The following lemma will be proved in § 26.

LEMMA. $\mathcal{K}(Q_* \otimes \wedge^s(\delta N)) = 0$ *for* $1 \leqq s \leqq r-d-1$.

Consequently, we have

$$\mathcal{K}(\operatorname{Ker}[\psi_*{}^s]) = \mathcal{K}(\operatorname{Im}[\psi_*{}^{s+1}]) \tag{9}$$

for $1 \leqq s \leqq r-d$ so that we obtain from (6), (7) and (9)

$$\mathcal{K}(Q_*) = \sum_{l=0}^{r-d} (-1)^l \mathcal{K}(F_*{}^l) \tag{10}$$

since $\mathrm{Im}[\psi_*{}^{r-d}] = F_*{}^{r-d}$.

Applying Proposition 4 of § 24, we obtain $\mathcal{K}(F^l) = \mathcal{K}(F_*{}^l)$ since $F_*{}^l$ is the reciprocal image of F^l with respect to the anti-monoidal transformation Φ from X^* onto X; similarly, we have $\mathcal{K}(Q) = \mathcal{K}(Q_*)$ since the restriction of Φ to V^* equips V^* with the structure of the dual projective bundle of $N = N(X;V)$ and Q_* is the reciprocal image of Q with respect to that restriction mapping. Thus (10) gives

$$\mathcal{K}(Q) = \sum_{l=0}^{r-d} (-1)^l \mathcal{K}(F^l). \tag{2}$$

SUPPLEMENT. *For any resolution*

$$0 \to F^t \to \cdots \to F^0 \to Q \to 0 \tag{11}$$

of Q by locally free sheaves $F^0, \cdots, F^t$ on X (t is necessarily $\geqq r-d$ as follows from Chap. II), *we have*

$$\mathcal{K}(Q) = \sum_{l=0}^{t} (-1)^l \mathcal{K}(F^l).$$

§ 26. THEOREM 6. *Let E be a locally free sheaf of dimension n defined on the non-singular projective model X. Then we have*

$$\mathfrak{a}(h\Theta(E) + \pi_E{}^*\vartheta) = \mathfrak{a}(X)$$

for all $1 \leqq h \leqq n-1$, where $\pi_E{}^*\vartheta$ is the reciprocal image with respect to π_E of any divisor class ϑ on X.

The proof will be by induction on the dimension n of the sheaf E. The theorem is vacuously true for $n=1$. Let $n>1$, and, as the inductive hypothesis, assume that the theorem is true for all locally free sheaves of dimension less than n. The main part of the proof is given in two lemmas.

LEMMA 1. *Theorem* 6 *is true under the further assumption that E admits an exact sequence*

$$0 \to D \xrightarrow{\phi} E \to F \to 0, \tag{1}$$

of locally free sheaves defined on X, where D is a locally free sheaf of dimension one.

Proof. We shall apply the results of § 17, Chap. III to the exact sequence (1). We have dim. $\mathcal{B}(F) = \text{dim.}\,\mathcal{B}(E) - 1$ since D is a locally free sheaf of dimension one defined on X; this proves that $\phi_{;1}$ is a bi-regular mapping $\mathcal{E}(\phi)$ onto $\mathcal{B}(E)$ since $\phi_{;1}$ is an anti-monoidal transformation whose center is the subvariety $\mathcal{B}(F)$ on $\mathcal{B}(E)$. In fact, here the dual projective transformation $\mathcal{B}(\phi)$ is a regular rational mapping from $\mathcal{B}(E)$ onto $\mathcal{B}(D) = X$ and $\mathcal{B}(\phi)$ is equal to the composite mapping $\phi_{;2} \circ \phi_{;1}^{-1}$ where $\phi_{;1}^{-1}$ is the inverse map to $\phi_{;1}$. The projection $\phi_{;2}$ equips $\mathcal{E}(\phi)$ with the structure of the dual projective bundle of a locally free sheaf of dimension n defined on $\mathcal{B}(D) = X$. On $\mathcal{E}(\phi)$, we have

$$(2) \qquad \phi_{;1}{}^*\Theta(E) = \phi_{;2}{}^*\Theta(D) + \Theta(S(\phi)),$$

where the divisor class $\Theta(S(\phi))$ contains the anti-center $\mathfrak{N}_\phi$, and of course $\phi_{;1}$ bi-regularly maps $\mathfrak{N}_\phi$ on $\mathcal{B}(F)$.

To avoid an unnecessarily pedantic notation, we shall identify $\mathcal{E}(\phi)$ with $\mathcal{B}(E)$ and $\mathfrak{N}_\phi$ with $\mathcal{B}(F)$ according to the mapping $\phi_{;1}$. Under this identification, the projection $\phi_{;2}$ is equal to π_E. Set $x = \phi_{;1}{}^*\Theta(E) = \Theta(E)$, $y = \phi_{;2}{}^*\Theta(D) = \pi_E{}^*\Theta(D)$, and $s = \Theta(S(\phi))$; hence s is the divisor class of $\mathcal{B}(F)$ on $\mathcal{B}(E)$ and we rewrite (2) as

$$(2') \qquad x = y + s.$$

The trace $\{x\}_{\mathcal{B}(F)}$ of x on $\mathcal{B}(F)$ is equal to $\Theta(F)$. From (2′), we have

$$(3) \qquad hx + \pi_E{}^*\vartheta = (h-1)x + y + \pi_E{}^*\vartheta + s,$$

where h is any integer $\geqq 1$ and ϑ is any divisor class on X. We have

$$(4) \qquad \mathfrak{a}(hx + \pi_E{}^*\vartheta) = \mathfrak{a}((h-1)x + y + \pi_E{}^*\vartheta) + \mathfrak{a}(s) - \mathfrak{a}(\{(h-1)x + y + \pi_E{}^*\vartheta\}_{\mathcal{B}(F)}),$$

as follows from Theorem 1 of § 22 since the divisor class s contains the non-singular member $\mathcal{B}(F)$.

Consider first the case where $h = 1$. Then (4) is simply

$$(5) \qquad \mathfrak{a}(x + \pi_E{}^*\vartheta) = \mathfrak{a}(y + \pi_E{}^*\vartheta) + \mathfrak{a}(s) - \mathfrak{a}(\{y + \pi_E{}^*\vartheta\}_{\mathcal{B}(F)}).$$

Now $y + \pi_E{}^*\vartheta$ (resp. $\{y + \pi_E{}^*\vartheta\}_{\mathcal{B}(F)}$) is the reciprocal image of $\Theta(D) + \vartheta$ with respect to π_E (resp. π_F) so that, from Theorem 2,

$$\mathfrak{a}(y + \pi_E{}^*\vartheta) = \mathfrak{a}(\Theta(D) + \vartheta) = \mathfrak{a}(\{y + \pi_E{}^*\vartheta\}_{\mathcal{B}(F)}).$$

Thus we have

$$\mathfrak{A}(x + \pi_E{}^*\vartheta) = \mathfrak{A}(s);$$

but $\mathfrak{A}(s) = \mathfrak{A}(\mathfrak{B}(F))$ since $\mathfrak{B}(F)$ belongs to s, and, from the Fiber Law, $\mathfrak{A}(\mathfrak{B}(F)) = \mathfrak{A}(X)$; this proves that

$$\mathfrak{A}(x + \pi_E{}^*\vartheta) = \mathfrak{A}(X).$$

Now assume that $h > 1$, $h \leqq n-1$ so that $1 \leqq h-1 \leqq n-2$. We have that F is a locally free sheaf of dimension $n-1$ defined on X and that

$$\{(h-1)x + y + \pi_E{}^*\vartheta\}_{\mathfrak{B}(F)} = (h-1)\Theta(F) + \pi_F{}^*\Theta(D) + \vartheta);$$

hence, by our inductive hypothesis, we have

$$\mathfrak{A}(\{(h-1)x + y + \pi_E{}^*\vartheta\}_{\mathfrak{B}(F)}) = \mathfrak{A}(X),$$

and since $\mathfrak{A}(s) = \mathfrak{A}(\mathfrak{B}(F)) = \mathfrak{A}(X)$, we obtain from (4) that

$$\mathfrak{A}(hx + \pi_E{}^*\vartheta) = \mathfrak{A}((h-1)x + y + \pi^*{}_E\vartheta).$$

Thus we have

$$\mathfrak{A}(hx + \pi_E{}^*\vartheta) = \mathfrak{A}(x + (h-1)y + \pi_E{}^*\vartheta), \tag{7}$$

and from the previous paragraph, we have that the right hand side of (7) is equal to $\mathfrak{A}(X)$. The proof of the lemma is complete.

We turn to the case where E is an arbitrary locally free sheaf of dimension n defined on X.

LEMMA 2. *Let $\Phi: Y \to X$ be a regular mapping from Y onto X which satisfies one of the conditions of the Fiber Law. If Theorem 6 is true for the reciprocal image sheaf ΦE of E with respect to Φ, then the theorem is true for the sheaf E.*

Proof. For we have that

$$h\Theta(\Phi E) + \pi_{\Phi E}{}^*(\Phi^*\vartheta) \tag{8}$$

is the reciprocal image of

$$h\Theta(E) + \pi_E{}^*\vartheta \tag{9}$$

with respect to the fiber preserving map from $\mathfrak{B}(\Phi E)$ onto $\mathfrak{B}(E)$ which covers the map $\Phi: Y \to X$ of the base spaces; the fiber preserving map satisfies one of the conditions of the Fiber Law since Φ is such a mapping; from Proposition 3 of § 22, we get that the virtual $\mathfrak{A}$-genera of (8) and (9) are

equal. But if Theorem 6 is true for ΦE, then the virtual $\mathcal{A}$-genus of (8) is equal to $\mathcal{A}(Y)$, and, from the Fiber Law, $\mathcal{A}(Y) = \mathcal{A}(X)$, which proves Theorem 6 for the sheaf E.

Completion of the proof of Theorem 6: Consider the sheaf ${}^{\#}E$ of § 4, Chap. I; it is a locally free sheaf of dimension n defined on the dual projective bundle $\mathcal{B}(\delta_{n-1}E)$ of the $(n-1)$-st derived sheaf $\delta_{n-1}E$ of E. The sheaf ${}^{\#}E$ is the reciprocal image of E with respect to the composite mapping

$$\Sigma = \pi_E \circ \pi_{\delta_1 E} \circ \cdots \circ \pi_{\delta_{n-2}E} \circ \pi_{\delta_{n-1}E}$$

from $\mathcal{B}(\delta_{n-1}E)$ onto X. The residue class sheaf of ${}^{\#}E$ modulo the subsheaf $\delta_{n-1}E$ is a locally free sheaf of dimension $n-1$ defined on $\mathcal{B}(\delta_{n-1}E)$, as follows from the composition series (4) of § 4, Chap. I. Thus Theorem 6 is true for ${}^{\#}E$ since ${}^{\#}E$ satisfies the addition assumption of Lemma 1. But Σ is composed of bundle projections of dual projective bundle so that by repeated application of Lemma 2, Theorem 6 is true for E since it is true for ${}^{\#}E$.

THEOREM 7. *E, F are locally free sheaves defined on X, and E is of dimension $n > 1$. Then we have*

$$\mathcal{K}(\pi_E F \otimes B^{-h}(E)) = 0$$

for all $1 \leqq h \leqq n-1$; ($B^{-1}(E)$ is such that $B^{-1}(E) \otimes B(E) = \mathcal{O}_{\mathcal{B}(E)}$ and $B^{-h}(E)$ is the tensor product of $B^{-1}(E)$ with itself h times).

Proof. Let T equal the dual projective bundle of the sheaf $\pi_E F$ defined on $\mathcal{B}(E)$; T is the induced fiber bundle of $\mathcal{B}(F)$ with respect to the mapping $\pi_E\colon \mathcal{B}(E) \to X$. Let $\xi_1\colon T \to \mathcal{B}(E)$ denote the bundle projection of T, and let $\xi_2\colon T \to \mathcal{B}(F)$ denote the fiber preserving map which covers the mapping $\pi_E\colon \mathcal{B}(E) \to X$ of the base spaces of T and $\mathcal{B}(F)$. It follows by inspection that ξ_2 equips T with the structure of the dual projective fiber bundle $\mathcal{B}(\pi_F E)$ of the sheaf $\pi_F E$ and that ξ_1 is the fiber preserving map from $T = \mathcal{B}(\pi_F E)$ onto $\mathcal{B}(E)$ which covers the mapping $\pi_F\colon \mathcal{B}(F) \to X$ of the base spaces of $\mathcal{A}(\pi_F E)$ and $\mathcal{B}(E)$. Thus we have that

$$\Theta(\pi_E F) = \xi_2{}^*\Theta(F),$$

$$\Theta(\pi_F E) = \xi_1{}^*\Theta(E).$$

The basic class of the sheaf $\pi_E F \otimes B^{-h}(E)$ is the divisor class

$$\Theta(\pi_E F \otimes B^{-h}(E)) = \Theta(\pi_E F) + \xi_1{}^*\Theta(B^{-h}(E))$$

on T, as follows from § 8 of Chap. I. But

$$\xi_1^*\Theta(B^{-h}(E)) = -h\xi_1^*\Theta(B(E)) = -h\xi_1^*\Theta(E),$$

which gives

$$\Theta(\pi_E F \otimes B^{-h}(E)) = \xi_2^*\Theta(F) - h\xi_1^*\Theta(E). \tag{10}$$

For $1 \leqq h \leqq n-1$, we can apply Theorem 6 to the sheaf $\pi_F E$ and obtain

$$\mathfrak{A}(h\xi_1^*\Theta(E) - \xi_2^*\Theta(F)) = \mathfrak{A}(\mathfrak{B}(F));$$

this is permissible since $\xi_1^*\Theta(E) = \Theta(\pi_F E)$, and $\pi_F E$ is a locally free sheaf of dimension n defined on $\mathfrak{B}(F)$. This proves, in virtue of (10), that

$$\mathfrak{A}(-\Theta(\pi_E F \otimes B^{-h}(E))) = \mathfrak{A}(\mathfrak{B}(F));$$

but

$$\mathcal{K}(\pi_E F \otimes B^{-h}(E)) = \mathfrak{A}(\mathfrak{B}(E)) - \mathfrak{A}(-\Theta(\pi_E F \otimes B^{-h}(E)))$$

and since $\mathfrak{A}(\mathfrak{B}(E)) = \mathfrak{A}(X) = \mathfrak{A}(\mathfrak{B}(F))$, our theorem follows.

The unproved lemma of § 25 is an immediate consequence of the following more general result.

THEOREM 8. *E, F are locally free sheaves as defined on X, and E is of dimension $n > 1$. Then*

$$\mathcal{K}(\pi_E F \otimes \wedge^s(\delta E)) = 0$$

for all $1 \leqq s \leqq n-1$; (recall that $\wedge^s(\delta E)$ is the s-fold exterior product of the derived sheaf δE of the sheaf E).

Proof. We rewrite the exact sequence (7) of § 5, Chap. I:

$$0\ \wedge^n(\pi_E E) \otimes B^{-(n-s)}(E) \to \cdots \to \wedge^{s+1}(\pi_E E) \otimes B^{-1}(E) \to \wedge^s(\delta E) \to 0.$$

It is an exact sequence of locally free sheaves defined on $\mathfrak{B}(E)$ and it is composed of the exact sequences

$$\begin{aligned} 0 \to \wedge^{s+k}(\delta E) \otimes B^{-k}(E) \to \wedge^{s+k}(\pi_E E) \otimes B^{-k}(E) \\ \to \wedge^{s+k-1}(\delta E) \otimes B^{-(k-1)}(E) \to 0 \end{aligned} \tag{11}$$

for $1 \leqq k \leqq n-s$. Tensorizing (11) with $\pi_E F$ preserves exactness since $\pi_E F$ is a locally free sheaf, and we obtain the exact sequences

$$\begin{aligned} 0 \to \pi_E F \otimes \wedge^{s+k}(\delta E) \otimes B^{-k}(E) \to \pi_E F \otimes \wedge^{s+k}(\pi_E E) \otimes B^{-k}(E) \\ \to \pi_E F \otimes \wedge^{s+(k-1)}(\delta E) \otimes B^{-(k-1)}(E) \to 0 \end{aligned} \tag{12}$$

for $1 \leqq k \leqq n-s$. From Theorem 3, we obtain

$$(13) \qquad \mathcal{K}(\pi_E F \otimes \wedge^s(\delta E)) = \sum_{k=1}^{n-s} (-1)^{k-1} \mathcal{K}(\pi_E F \otimes \wedge^{s+k}(\pi_E E) \otimes B^{-k}(E))$$

since $\wedge^n(\delta E)$ is the sheaf zero (δE is of dimension $n-1$). On the other hand,

$$\pi_E F \otimes \wedge^{s+k}(\pi_E E) = \pi_E(F \otimes \wedge^{s+k}(E))$$

and from Theorem 7, we have

$$\mathcal{K}(\pi_E(F \otimes \wedge^{s+k}(E)) \otimes B^{-k}(E)) = 0$$

for all $1 \leqq k \leqq n-s$; thus we finally have

$$\mathcal{K}(\pi_E F \otimes \wedge^s(\delta E)) = 0.$$

§ 27. $K[X_0, \cdots, X_r]$ is the ring of polynomials in the $r+1$ indeterminates $X_0, \cdots, X_r$ with coefficients in the fixed field K. By an S-module (terminology of Koszul, Serre, $\cdots$), we mean simply a module $\mathfrak{M}$ over the ring $S = K[X_0, \cdots, X_r]$. All S-modules considered here are unitary, graded, and finitely generated by homogeneous elements.

Unitary: this means $1 \cdot m = m$ for all $m \in \mathfrak{M}$, where 1 is the constant polynomial 1 in $K[X_0, \cdots, X_r]$.

Graded: $\mathfrak{M}$ is equal to a direct sum of additive subgroups $\mathfrak{M}^k$, $0 \leqq k < \infty$; the elements of $\mathfrak{M}^k$ are called homogeneous of degree k and we require that $Fm \in \mathfrak{M}^{h+k}$ for a homogeneous polynomial F of degree h and $m \in \mathfrak{M}^k$.

Finitely generated by homogeneous elements: it is possible to choose finitely many homogeneous elements $m_1, \cdots, m_t$ from $\mathfrak{M}$ which generate $\mathfrak{M}$ as module over $K[X_0, \cdots, X_r]$; this implies that $\mathfrak{M}^k$ is a finite dimensional vector space over the field K; $m_1, \cdots, m_t$ is called a system of generators of $\mathfrak{M}$.

By a homomorphism $\Psi: \mathfrak{M} \to \mathfrak{N}$ of S-modules $\mathfrak{M}$, $\mathfrak{N}$, we shall mean a homomorphism of their structure as modules over $K[X_0, \cdots, X_r]$ that preserves degree; that is Ψ maps $\mathfrak{M}^k$ into $\mathfrak{N}^k$ for all $0 \leqq k < \infty$. It is easy to check that $\mathrm{Ker}[\Psi: \mathfrak{M} \to \mathfrak{N}]$ and $\mathrm{Im}[\Psi: \mathfrak{M} \to \mathfrak{N}]$ are sub S-modules of $\mathfrak{M}$ and $\mathfrak{N}$ respectively. $\mathfrak{M}$ is called a "free" S-module if we can choose a (homogeneous) system of generators of $\mathfrak{M}$ which generate $\mathfrak{M}$ as a free module over $K[X_0, \cdots, X_r]$.

Let $\mathfrak{M}$ be any S-module. Since $\mathfrak{M}$ is finitely generated, it is possible to choose a free S-module $\mathfrak{F}_0$ and a homomorphism Ψ_0 from $\mathfrak{F}_0$ onto $\mathfrak{M}$ so that we have the exact sequence of S-modules

$$0 \to \mathrm{Ker}[\Psi_0] \to \mathfrak{F}_0 \to \mathfrak{M} \to 0.$$

Repeating this process several times, we arrive at an exact sequence of S-modules

$$\mathcal{F}_t \xrightarrow{\Psi_t} \mathcal{F}_{t-1} \to \cdots \to \mathcal{F}_0 \to \mathfrak{M} \to 0,$$

where $\mathcal{F}_0, \cdots, \mathcal{F}_t$ are free S-modules. Hilbert's famous theorem on "chains of syzygies" asserts that $\operatorname{Ker}[\Psi_t]$ is a free S-module if $t \geqq r$. Thus, for any S-module $\mathfrak{M}$, it is possible to construct an exact sequence

$$(1) \qquad 0 \to \mathcal{F}_r \xrightarrow{\Psi_r} \mathcal{F}_{r-1} \to \cdots \xrightarrow{\Psi_1} \mathcal{F}_0 \xrightarrow{\Psi_0} \mathfrak{M} \to 0,$$

where $\mathcal{F}_0, \cdots, \mathcal{F}_r$ are free S-modules.

For any h, $0 \leqq h < \infty$, we have the exact sequence of vector spaces

$$0 \to \mathcal{F}_r^h \to \cdots \to \mathcal{F}_s^h \to \cdots \to \mathcal{F}_0^h \to \mathfrak{M}^h \to 0,$$

where $\mathfrak{M}^h$ (resp. $\mathcal{F}_s^h$) is the vector space over K consisting of the homogeneous elements of degree h of $\mathfrak{M}$ (resp. $\mathcal{F}_s$). For the dimensions of these vector spaces, we have the relation

$$\dim. \mathfrak{M}^h = \sum_{s=0}^{r} (-1)^s \dim. \mathcal{F}_s^h.$$

Now for all $h \gg 0$ (that is for all sufficiently large h), we have

$$\dim. \mathcal{F}_s^h = \chi(\mathcal{F}_s; h),$$

where $\chi(\mathcal{F}_s; h)$ is a polynomial in h with rational coefficients; this is obvious if we recall that each $\mathcal{F}_s$ is a free S-module. Set

$$\chi(\mathfrak{M}; h) = \sum_{s=0}^{r} (-1)^s \chi(\mathcal{F}_s; h).$$

Then $\chi(\mathfrak{M}; h)$ is a polynomial in h with rational coefficients and we have that for $h \gg 0$,

$$\dim. \mathfrak{M}^h = \chi(\mathfrak{M}; h).$$

$\chi(\mathfrak{M}; h)$ is called the Hilbert characteristic polynomial of the S-module $\mathfrak{M}$; and we have repeated Hilbert's own proof of its existence.

§ 28. P^r $(=P)$ is a projective space of dimension r, and let us identify $K[X_0, \cdots, X_r]$ with the homogeneous coordinate ring over K of P. Serre has given a method whereby one associates with any S-module $\mathfrak{M}$ a (coherent, algebraic) sheaf M defined on P. We shall review his construction first for the special case of a free S-module $\mathcal{F}$. The associated sheaf F is then a

locally free sheaf defined on P. For let $f_1, \cdots, f_n$ freely generate $\mathfrak{F}$, so that $f_1, \cdots, f_n$ are homogeneous elements say of degrees $h_1, \cdots, h_n$ respectively; let $\{U_\alpha\}$, $\alpha = 0, 1, \cdots, r$, be the standard covering of P, that is U_α is the open set on P whose frontier is the hyperlane $X_\alpha = 0$. The restriction of F to any U_α is a free sheaf generated by sections $f^\alpha{}_1, \cdots, f^\alpha{}_n$ of F over U_α; on $U_\alpha \cap U_\beta$, we have the transition laws

$$f^\alpha{}_i = (X_\beta / X_\alpha)^{h_i} f^\beta{}_i, \qquad 1 \leqq i \leqq n,$$

(h_i is the degree of the generator f_i). It is evident that the associated sheaf F is equal to the direct sum of the sheaves $\mathcal{O}(-h_1), \cdots, \mathcal{O}(-h_n)$. ($\mathcal{O}(-h)$ is isomorphic to the sheaf $\mathcal{L}(\vartheta_h)$ of germs of rational functions on P which are multiples of a divisor ϑ_h belonging to the linear system of hypersurface sections of order h on P.)

A locally free sheaf defined on P is called "S-free" if it is the associated sheaf of a free S-module; it is clear that a sheaf is S-free if and only if it is a direct sum of finitely many sheaves of type $\mathcal{O}(-h)$ with $h \geqq 0$.

Let $\mathfrak{G}$ be a free S-module, and let there be a homomorphism $\Psi \colon \mathfrak{G} \to \mathfrak{F}$. Then there is an associated sheaf homomorphism $\psi \colon G \to F$ of the associated S-free sheaves. Let Ψ be described by

$$\Psi \colon g_p \to \sum_{i=1}^{n} A_{i,p} f_i, \qquad 1 \leqq p \leqq m$$

(assume that $\mathfrak{G}$ has m generators), where the A's are homogeneous polynomials and

$$\deg. g_p = \deg. A_{i,p} + \deg. f_i$$

for all $1 \leqq i \leqq n$. The restriction of the sheaf homomorphism $\psi \colon G \to F$ to any U_α is described by

$$g_p{}^\alpha \to \sum_{i=1}^{n} (A_{i,p} / (X_\alpha)^{\nu_{i,p}}) f^\alpha{}_i, \qquad 1 \leqq p \leqq m,$$

where $\nu_{i,p} = \deg. A_{i,p}$.

Let $\mathfrak{M}$ be any S-module, and choose free S-modules $\mathfrak{F}$, $\mathfrak{G}$ and homomorphisms $\Psi' \colon \mathfrak{F} \to \mathfrak{M}$, $\Psi \colon \mathfrak{G} \to \mathfrak{F}$ such that

$$\mathfrak{G} \xrightarrow{\Psi} \mathfrak{F} \xrightarrow{\Psi'} \mathfrak{M} \to 0$$

is an exact sequence of S-modules. The associated sheaf M of $\mathfrak{M}$ is defined to be the residue class sheaf $F/\mathrm{Im}[\psi]$, where $\mathrm{Im}[\psi]$ is the image of G by the

associated homomorphism $\psi\colon G\to F$; it is easy to check that M depends solely on $\mathfrak{M}$ and that there is an associated sheaf homomorphism $\psi'\colon F\to M$ so that we have the exact sequence of sheaves

$$G\xrightarrow{\psi}F\xrightarrow{\psi'}M\to 0.$$

For an arbitrary S-module $\mathfrak{M}$, we recopy the "chain of syzygies" (1) of the preceding §:

$$0\to\mathfrak{F}_r\xrightarrow{\Psi_r}\cdots\xrightarrow{\Psi_1}\mathfrak{F}_0\xrightarrow{\Psi_0}\mathfrak{M}\to 0. \tag{1}$$

Applying Serre's construction, we take associated sheaves and homomorphisms and we have the exact sequence of sheaves

$$0\to F_r\xrightarrow{\psi_r}\cdots\xrightarrow{\psi_1}F_0\xrightarrow{\psi_0}M\to 0, \tag{2}$$

where $F_0,\cdots,F_r$ are S-free sheaves. According to Serre's cohomology theory, we have the Euler-Poincaré characteristic $\chi(P,M)$ of the sheaf M, where

$$\chi(P,M)=\sum_{t=0}^{\infty}(-1)^t\dim.H^t(P,M)$$

($H^t(P,M)$ is the t-dimensional cohomology module of the sheaf M defined on P). We also have that

$$\chi(P,M)=\sum_{s=0}^{r}(-1)^s\chi(P,F_s). \tag{3}$$

Incidentally, Serre has proved that

$$\chi(P,M)=\chi(\mathfrak{M},0),$$

that is, where $\chi(\mathfrak{M},0)$ is the value of the Hilbert characteristic polynomial of $\mathfrak{M}$ for $h=0$.

Let V be a non-singular subvariety on P, and let $\mathfrak{R}(V)$ be the homogeneous coordinate ring of V, that is $\mathfrak{R}(V)$ is the residue class ring of $K[X_0,\cdots,X_r]$ modulo the ideal determined by V. Then $\mathfrak{R}(V)$ is an S-module. The associated sheaf of $\mathfrak{R}(V)$ is easily seen to be the sheaf $\mathcal{O}_V$ of local rings of V extended to P. From (2), we get, upon setting $M=\mathcal{O}_V$, the exact sequence

$$0\to F_r\xrightarrow{\psi_r}\cdots\xrightarrow{\psi_1}F_0\xrightarrow{\psi_0}\mathcal{O}_V\to 0, \tag{4}$$

where $F_0, \cdots, F_r$ are S-free sheaves. From the Supplement to Theorem 5 of § 25, we obtain that

$$\mathcal{K}(\mathcal{O}_V) = \sum_{s=0}^{r} (-1)^s \mathcal{K}(F_s). \tag{5}$$

In the next §, we shall prove that $\mathcal{K}(F) = \chi(P, F)$ for an S-free sheaf F. On the basis of this assertion, we obtain from (3) and (5) that

$$\chi(V, \mathcal{O}_V) = \mathcal{K}(\mathcal{O}_V).$$

Since $\mathcal{K}(\mathcal{O}_V) = \mathfrak{a}(V)$, we have proved the unicity $\mathfrak{a}$, for we now have:

THEOREM 9. *Let V be a non-singular projective model. Then we have*

$$\mathfrak{a}(V) = \chi(V, \mathcal{O}_V).$$

§ 29. PROPOSITION 5. *Let F be an S-free sheaf. Then $\mathcal{K}(F) = \chi(P; F)$.* (This proposition completes the proof of Theorem 9.)

Proof. F, since it is S-free, is equal to a direct sum

$$\mathcal{O}(-h_1 + \cdots + \mathcal{O}(-h_n)$$

with each $h_i \geqq 0$. Now, from the Serre cohomology theory, we have

$$\chi(P; F) = \sum_{t=1}^{n} \chi(P; \mathcal{O}(-h_t)),$$

and, from Theorem 3, we have

$$\mathcal{K}(F) = \sum_{t=1}^{n} \mathcal{K}(\mathcal{O}(-h_t)).$$

Hence it suffices to prove our proposition merely for sheaves of type $\mathcal{O}(-h)$, $h \geqq 0$.

Proposition 5 follows from:

PROPOSITION 6. $\mathcal{K}(\mathcal{O}(-h)) = \chi(P, \mathcal{O}(-h)) \quad (h \geqq 0)$.

Proof. The proof is by induction on the dimension r of P and the degree h. We assume that our proposition is true for S-free sheaves of dimension one defined on projective spaces of dimension less than r. (It is clearly true for a projective space of dimension zero.) For the case $h = 0$ on P, it is true; (it is well known that

$$\chi(P; \mathcal{O}_P) = 1,$$

$\mathcal{O}_P = \mathcal{O}(0)$, and $\mathcal{K}(\mathcal{O}_P) = \mathfrak{a}(P) = 1$ by the Normalization Axiom). Therefore, we assume that $h > 0$ and that our proposition is true for $h - 1$. Consider the exact sequence

$$0 \to \mathcal{O}(-h) \to \mathcal{O}(-(h-1)) \to \mathcal{O}_{P'}(-(h-1)) \to 0;$$

P' is a projective subspace of dimension $r-1$ on P and $\mathcal{O}_{P'}(-(h-1))$ is the extension to P of an S-free sheaf defined on P'. From the Serre cohomology theory, we have

(1) $$\chi(P; \mathcal{O}(-h)) = \chi(P; \mathcal{O}(-(h-1))) - \chi(P', \mathcal{O}_{P'}(-(h-1))),$$

and from Theorem4, we have

(2) $$\mathcal{K}(\mathcal{O}(-h)) = \mathcal{K}(\mathcal{O}(-(h-1))) - \mathcal{K}(\mathcal{O}_{P'}(-(h-1))).$$

From our inductive assumption, we obtain that the right hand sides of (1) and (2) are equal, which proves

$$\mathcal{K}(\mathcal{O}(-h)) = \chi(P; \mathcal{O}(-h)).$$

THE JOHNS HOPKINS UNIVERSITY.

A DUALITY THEORY FOR INJECTIVE MODULES.*

(Theory of Quasi-Frobenius Modules)

By Goro Azumaya.[1]

Introduction. Let A be a finite-dimensional algebra with identity element over a field Φ. Let M be a finitely generated left A-module. Then M, when regarded as a left representation space, defines a representation of A in Φ, and there corresponds to this representation a finitely generated right A-modul M^*, which is called the dual representation space of M. M^* is nothing but the conjugate space of M, i. e., the vector space consisting of all Φ-linear mappings f of M into Φ, where fa, $a \in A$, is defined to be the mapping $x \rightarrow f(ax)$, $x \in M$, and moreover we have, by associating M with M^*, a one-to-one correspondence (up to isomorphisms) between finitely generated left and right A-modules. The present paper establishes a theory which extends this known situation to the case where A is a ring with minimum condition and possessing a certain type of injective module, so that it provides also a generalization of the theory of quasi-Frobenius rings, which has been developed mainly by T. Nakayama, M. Hall and M. Ikeda. Our principal results are summarized as follows:

Let A be a ring with identity element and satisfying the left minimum condition.[2] Suppose that Q is a finitely generated left A-module which is injective and contains an isomorphic image of every irreducible left A-module. Let A^* be the A-endomorphism ring of Q, considered as a right operator-ring. Then we have first that the same situations hold quite symmetrically for the A^*-module Q, that is, A^* satisfies the right minimum condition, Q is, as right A^*-module, both finitely generated and injective and contains an isomorphic image of every irreducible right A^*-module, and moreover A coincides with the A^*-endomorphism ring of Q (Theorem 6). Now, let M be a left A-module. We consider the module $M^* = \mathrm{Hom}_A(M, Q)$ consisting of all

* Received November 19, 1857; revised October 6, 1958.

[1] This work was supported by the Office of Naval Research, under Contract Nonr 609-19.

[2] By left minimum (or maximum) condition we mean the minimum (or maximum) condition for left ideals. As is well-known, the left minimum condition implies always the left maximum condition, under the assumption of the existence of identity element.

A-homomorphisms f of M into Q. M^* can be converted into a right A^*-module by defining fa^*, $a^* \in A^*$, to be the mapping $x \to f(x)a^*$, $x \in M$, which we shall call the dual module of M (with respect to Q).[3] Similarly, we may define a dual module for every right A^*-module. We have then the following fundamental duality theorem: Let M be a finitely generated left A-module. Then its dual module M^* is also finitely generated, and moreover, M may be regarded as the dual module of M^* in the natural way. The same holds also for every finitely generated right A^*-module (Theorem 8). Let now M_1 and M_2 be two finitely generated left A-modules and let M_1^* and M_2^* be their respective dual modules. Then with each A-homomorphism ϕ of M_1 into M_2 we can associate, in the usual manner, its dual mapping ϕ^* which is an A^*-homomorphism of M_2^* into M_1^*, and in this case, ϕ is regarded, by virtue of the above duality theorem, as the dual mapping of ϕ^*. We have thus an isomorphism $\phi \leftrightarrow \phi^*$ between the groups $\mathrm{Hom}_A(M_1, M_2)$ and $\mathrm{Hom}_{A^*}(M_2^*, M_1^*)$. Further, it is clear that if ψ is an A-homomorphism of M_2 into a third finitely generated left A-module, then $(\psi\phi)^* = \phi^*\psi^*$.

Interesting is however the fact that a complete converse of these situations holds in the following form: Let A and A^* be two rings with identity elements (but not be assumed to satisfy any chain conditions). Suppose that there is associated with each finitely generated left A-module M a finitely generated right A^*-module M^* so that the M^*'s exhaust, up to isomorphisms, all finitely generated right A^*-modules. Suppose furthermore that for each pair of finitely generated left A-modules M_1 and M_2 there is given an isomorphism $\phi \leftrightarrow \phi^*$ of $\mathrm{Hom}_A(M_1, M_2)$ onto $\mathrm{Hom}_{A^*}(M_2^*, M_1^*)$ in such a way that these isomorphisms together fulfill $(\psi\phi)^* = \phi^*\psi^*$. Then A and A^* indeed satisfy the left and right minimum conditions respectively, and we can find a two-sided A-A^*-module Q such that Q, when regarded as a left A-module, is of the same type as above and A^* coincides with its A-endomorphism ring, and moreover every M^* may be so identified with the dual module of M with respect to Q that every ϕ^* coincides with the dual mapping of ϕ (Theorem 10).

In order to establish the above results, it is indispensable to make use of an important concept of quasi-Frobenius two-sided modules for two rings A and A^*, which was however essentially introduced in the recent paper of Morita and Tachikawa [9], and in fact our theory should also be regarded as a theory of such modules. In particular, [9, Theorem 1.1], in a generalized

[3] Here and hereafter, one should pay attention to the fact that A^* is not necessarily (isomorphic to) the dual module of the left A-module A. Whenever there is a fear of such confusion, we shall use the notation A_r for the left (or right) A-module A.

form, plays a basic role. It turns out, among other things, that under the respective assumptions of the left and the right minimum conditions for A and A^*, quasi-Frobenius modules are exactly the same as the above considered modules Q, when regarded as two-sided A-A^*-modules, and moreover a ring A satisfying the left or the right minimum condition is a quasi-Frobenius ring if and only if it is quasi-Frobenius as a two-sided A-module. On the other hand, it may be of some interest that the notion of quasi-Frobenius modules gives a natural extension of the density theorem for irreducible modules and completely reducible modules. In fact, it will be shown in particular that a necessary and sufficient condition for a two-sided A-A^*-module, which is both faithful and completely reducible with respect to A, to be quasi-Frobenius is that A^* is a dense subring of the A-endomorphism ring of the module. Furthermore, we shall, in the last section, apply the above theory to algebras over a commutative ring with minimum condition to make it possible, for instance, to verify for the first time that the symmetricity of an algebra over a field is entirely independent of the choice of the base field.

It should be noted, in this connection, that a ring A with the left minimum conditions does not always possess an injective left module Q of the above mentioned type, as has recently been shown by Rosenberg and Zelinsky [14], while every finite-dimensional algebra A as well as every quasi-Frobenius ring A certainly has such a module.

Needless to say, the present study is indebted much to the fundamental works of Nakayama [11, 12] and Ikeda [5]. Also, I wish to express my thanks to Professor N. Jacobson who let me have an opportunity to discuss fully about the present subject in his seminar, as well as to Professors A. Rosenberk and D. Zelinsky who have communicated to me valuable information on the existence of injective modules during the preparation of this paper.

1. **Preliminaries.** Throughout this paper we shall assume, unless otherwise stated, that all rings considered have identity elements and also all (left, right, or two-sided) modules over rings are unital in the sense that identity elements operate on the modules as identity (cf. Jacobson [7, p. 1]).

Let A be a ring. A left A-module Q is, following Cartan and Eilenberg [1], called *injective* with respect to A (or A-injective) if given an left A-module M, an A-submodule M' and an A-homomorphism $f': M' \rightarrow Q$, there is an extension A-homomorphism $f: M \rightarrow Q$. We may however restrict our-

selves here to the particular case where $M = A$, as a matter of fact ([1, Theorem I. 3. 2]). Now, in order that Q be injective it is necessary and sufficient that Q be a direct summand in every extension A-module. In fact, we have more strongly the following

PROPOSITION 1. *A left A-module Q is injective if (and only if) Q is a direct summand in every extension A-module which is expressible as a sum of Q and a cyclic A-submodule.*

Proof. Let $\mathfrak{l}$ be a left ideal of A and f an A-homomorphism of $\mathfrak{l}$ into Q. Let $M = A \oplus Q$ be the direct sum of two left A-modules A and Q. Then all elements of the form $(a, -f(a))$ with $a \in \mathfrak{l}$ constitute an A-submodule M' of M. We consider the factor module $M'' = M - M'$. By identifying $u \in Q$ with the coset of $(0, u)$ modulo M', Q is clearly imbedded isomorphically into M''. Furthermore, A is, by associating $a \in A$ with the coset of $(a, 0)$, mapped homomorphically onto a (cyclic) submodule of M'', and so M'' is a sum of Q and this submodule. Consequently, M'' may be expressed as a direct sum of Q and a second submodule. Let v be the Q-component of the coset of $(1, 0)$ relative to this direct decomposition. Then we have immediately $av = f(a)$ for every $a \in \mathfrak{l}$, which shows that Q is injective.

COROLLARY. *If Q is a finitely generated left A-module, then Q is injective if and only if Q is a direct summand in every finitely generated extension A-module of Q.*

Now let Q be any left A-module. Consider a maximal left ideal $\mathfrak{l}$ of A. One can easily see that Q contains a minimal A-submodule which is A-isomorphic to the irreducible factor module $A - \mathfrak{l}$ if and only if the right annihilator $r_Q(\mathfrak{l})$ of $\mathfrak{l}$ in Q is non-zero, and in fact, when this is the case, cyclic submodules Au with non-zero elements u in $r_Q(\mathfrak{l})$ and only those are isomorphic images of $A - \mathfrak{l}$ in Q. On the other hand, if $\mathfrak{m}$ is an irreducible A-submodule of Q and if u is any non-zero element in $\mathfrak{m}$ then the left annihilator $l(u) = l_A(u)$ of u in A is a maximal left ideal of A and $\mathfrak{m} = Au$ is isomorphic to $A - l(u)$. These facts mean that the (A-)socle of Q, i. e., the sum of all irreducible A-submodules of Q coincides with the sum of the $r_Q(\mathfrak{l})$'s for all maximal left ideals $\mathfrak{l}$ of A. Moreover, for any given maximal left ideal $\mathfrak{l}$ of A such that Q contains an isomorphic image of $A - \mathfrak{l}$, the homogeneous component of the socle belonging to the irreducible left A-module $A - \mathfrak{l}$ (cf. [7, p. 63]) may be expressed not only in the form $Ar_Q(\mathfrak{l})$ but also as the sum of the $r_Q(\mathfrak{l}')$'s for all those maximal left ideals $\mathfrak{l}'$

for which $A - \mathfrak{l}'$ is isomorphic to $A - \mathfrak{l}$. We now call Q *distinguished* with respect to A (or A-distinguished) if Q contains an isomorphic image of every irreducible left A-module, or equivalently, if $r_Q(\mathfrak{l}) \neq 0$ for all maximal left ideals $\mathfrak{l}$ of A. Because of the fact that every proper left ideal is contained in a maximal left ideal, it is clear that Q is distinguished if and only if $r_Q(\mathfrak{l}) \neq 0$ for all proper left ideals $\mathfrak{l}$ of A. Further, we shall call Q *weakly distinguished* if, for any A-submodules $\mathfrak{m}$ and $\mathfrak{m}'$ of Q such that $\mathfrak{m} \supset \mathfrak{m}'$ and the factor module $\mathfrak{m} - \mathfrak{m}'$ is irreducible, Q contains an isomorphic image of $\mathfrak{m} - \mathfrak{m}'$. Evidently, distinguishedness implies weak distinguishedness.

Finally, we shall mean by the *capacity* of any irreducible left A-module the (finite or infinite) dimension of it over its endomorphism division ring.

2. Quasi-Frobenius modules. We consider, besides A, a second ring A^*, and suppose that Q is a two-sided A-A^*-module (in the sense that Q is a left A- and a right A^*-module at the same time and $(au)a^* = a(ua^*)$ for every $a \in A$, $u \in Q$, $a^* \in A^*$). Let M be a left A-module, and let $M^* = \mathrm{Hom}_A(M, Q)$ be the module consisting of all A-homomorphisms of M into Q. For any $x \in M$ and $f \in M^*$, we denote by xf the image of x by f. M^* can be made into a right A^*-module by setting $x(fa^*) = (xf)a^*$, $a^* \in A^*$, which we shall call the *right-dual module* of M with respect to Q. Similarly, we may define a *left-dual module* for any right A^*-module. Now, we call Q a *quasi-Frobenius two-sided A-A^*-module* if i) Q is faithful (with respect to both A and A^*), and ii) for every maximal left ideal $\mathfrak{l}$ of A and for every maximal right ideal $\mathfrak{r}$ of A^* the right annihilator $r_Q(\mathfrak{l})$ and the left annihilator $l_Q(\mathfrak{r})$ of $\mathfrak{l}$ and $\mathfrak{r}$ in Q are A^*-irreducible and A-irreducible respectively unless they are zero. If we observe however that for any left ideal $\mathfrak{l}$ of A the right annihilator $r_Q(\mathfrak{l})$ may be regarded as the right-dual module of $A - \mathfrak{l}$ and the similar holds for every right ideal, we may evidently replace the second condition ii) by the following: ii′) the right-dual module of every irreducible left A-module as well as the left-dual module of every irreducible right A^*-module, both with respect to Q, is irreducible whenever it is non-zero (or equivalently, whenever Q contains an isomorphic image of the given irreducible module).

THEOREM 1. *Let Q be a quasi-Frobenius two-sided A-A^*-module. Then the A-socle of Q coincides with the A^*-socle of Q. Moreover, if M is an irreducible left A-module such that Q contains an isomorphic image of M, or equivalently, the right-dual module M^* of M is irreducible, then the homogeneous (A-)component of the common socle belonging to M and the*

homogeneous (A^*-)component belonging to M^* coincide and it is a minimal A-A^*-submodule.

Proof. The homogeneous A-component of the A-socle belonging to M is the sum of the $r_Q(\mathfrak{l})$'s for all those maximal left ideals $\mathfrak{l}$ of A for which $A-\mathfrak{l}$ are isomorphic to M (§1). Such $r_Q(\mathfrak{l})$'s are however all (A^*-)isomorphic to M^*, and so the A-component is contained in the homogeneous A^*-component of the A^*-socle belonging to M^*. Since M is obviously the left-dual of M^*, we can conclude by symmetry that both the components coincide. Now, for a fixed maximal left ideal $\mathfrak{l}$ as above, any non-zero A-submodule of the common component contains a non-zero element of $r_Q(\mathfrak{l})$, because it contains an isomorphic image of $M \cong A-\mathfrak{l}$. This, together with the A^*-irreducibility of $r_Q(\mathfrak{l})$, implies that any non-zero A-A^*-submodule of the component contains $Ar_Q(\mathfrak{l})$, whereas the latter coincides with the component itself (§1), which shows nothing but the minimality of the component as a two-sided A-A^*-module. The coincidence of socles follows immediately from that of homogeneous components.

Let M be a left A-module and M^* a right A^*-module. Suppose that for any $x \in M$ and $y \in M^*$ there is defined a product xy in Q satisfying the following conditions, for $x, x' \in M$, $y, y' \in M^*$, $a \in A$, $a^* \in A^*$:

$$(x+x')y = xy + x'y, \qquad x(y+y') = xy + xy'$$
$$(ax)y = a(xy), \qquad (xy)a^* = x(ya^*).$$

If moreover $xM^* = 0$, $x \in M$, and $My = 0$, $y \in M^*$, imply always $x = 0$ and $y = 0$, then we shall, following Morita and Tachikawa [9], say that M and M^* form an *orthogonal pair* with respect to Q (and relative to the given product).[4] Now we have, as a generalization of [9, Theorem 1.1], the following fundamental

PROPOSITION 2. *Let Q be a quasi-Frobenius two-sided A-A^*-module. Suppose that a left A-module M and a right A^*-module M^* form an orthogonal pair with respect to Q, and suppose further that either M or M^* satisfies both the maximum and the minimum conditions for A- or A^*-submodules respectively. Then the other one also satisfies the same conditions, and moreover M and M^* may be regarded, in the natural manner, as the left-dual and the right-dual modules of M^* and M respectively.*

[4] In [9], the notion was defined in the special case where $A = A^*$. In this connection, the concept of dual modules was also introduced in this case, by the name of character modules.

The proof is virtually the same as that in the above cited theorem in [9], but we shall state it here for completeness. We may assume, without loss of generality, that M satisfies both the maximum and the minimum conditions, or equivalently, M has a composition series for A-submodules, say

$$M = M_0 \supset M_1 \supset \cdots \supset M_{s-1} \supset M_s = 0.$$

Consider then the following series of A^*-submodules of M^*:

$$M^* = r(M_s) \supseteqq r(M_{s-1}) \supseteqq \cdots \supseteqq r(M_1) \supseteqq r(M_0) = 0,$$

where $r(M_i)$ denotes, for each i, the right annihilator of M_i in M^*. The right multiplication of each element of $r(M_i)$ clearly induces in $M_{i-1} - M_i$ an A-homomorphism into Q and moreover elements of $r(M_{i-1})$ and only these induce the zero-mapping. Therefore $r(M_i) - r(M_{i-1})$ may be regarded as an A^*-submodule of the right-dual module of $M_{i-1} - M_i$. But since $M_{i-1} - M_i$ is irreducible and since Q is quasi-Frobenius, the right-dual of $M_{i-1} - M_i$ is either irreducible or zero, so that $r(M_i) - r(M_{i-1})$ is irreducible unless $r(M_i) = r(M_{i-1})$. It turns out from this that M^* has a composition series whose length $[M^*]_r$ does not exceed the composition length $s = [M]_l$ of M. Then we should, by symmetry, conclude that $[M]_l = [M^*]_r$. Now, M^* may be looked upon, in the natural manner, as an A^*-submodule of the right-dual module $\mathrm{Hom}_A(M, Q)$ of M. Therefore, M and $\mathrm{Hom}_A(M, Q)$ form also an orthogonal pair, and the later posesses a composition series whose length is equal to $[M]_l = [M^*]_r$. This implies that $M^* = \mathrm{Hom}_A(M, Q)$. Similarly, we have $M = \mathrm{Hom}_{A^*}(M^*, Q)$.

COROLLARY. *Under the same assumption as in Proposition 2, A-submodules L of M and A^*-submodules R of M^* correspond one-to-one by the following relations:*

$$r(L) = R, \qquad L = l(R),$$

where $r(\ )$ and $l(\ )$ mean the right and the left annihilators in M^* and M respectively; and, in this case, L and $M^* - R$, $M - L$ and R may respectively be regarded as dual modules of each other.

Proof. Let L be an A-submodule of M. Then L and $M^* - r(L)$ form naturally an orthogonal pair, so that L may be regarded as the left-dual module of the latter. But since $r(L)$ is also the right annihilator of $l(r(L))$, $l(r(L))$ is the left-dual module of $M^* - r(L)$ too. This implies, because of $L \subseteq l(r(L))$, that $L = l(r(L))$. Similarly, we have $R = r(l(R))$ for any A^*-submodule R of M^*.

Proposition 3. *Let Q be a faithful two-sided A-A^*-module. In order that Q be quasi-Frobenius it is necessary and sufficient that the A-socle of Q contain the A^*-socle of Q and every A-homomorphism of any finitely generated completely reducible A-submodule of Q into Q can be given by the right multiplication of an element of A^*.*

Proof. Suppose that Q is quasi-Frobenius. That the A-socle contains (and in fact coincides with) the A^*-socle follows from Theorem 1. Let now L be a finitely generated completely reducible A-submodule of Q. Then L satisfies both the maximum and the minimum conditions. On the other hand, the left A-module L and the right A^*-module $A^*-r(L)$, $r(L)$ being the right annihilator of L in A^*, form an orthonal pair. Hence the latter may, by Proposition 2, be regarded as the right-dual module of L, or what is the same thing, every A-homomorphism of L into Q can be obtained by right-multiplying an element of A^*.

To prove the sufficiency, consider first a maximal left ideal $\mathfrak{l}$ of A such that $r_Q(\mathfrak{l}) \neq 0$. Take two non-zero elements u, v from $r_Q(\mathfrak{l})$. Then, by associating au, $a \in A$, with av, we have an A-isomorphism of Au onto Av, both of which are irreducible A-submodules isomorphic to $A-\mathfrak{l}$. The isomorphism may, therefore, be given by the right multiplication of an element a^* of A^*: $ua^* = v$, and this shows that $l_Q(\mathfrak{l})$ is A^*-irreducible. Consider next a maximal right ideal $\mathfrak{r}$ of A^* such that $r_Q(\mathfrak{r}) \neq 0$. Then $l_Q(\mathfrak{r})$ is contained in the (A^*- whence) A-socle and so it is a completely reducible A-submodule. Suppose that $l_Q(\mathfrak{r})$ were not irreducible. Then it would contain two distinct irreducible A-submodules $\mathfrak{m}$ and $\mathfrak{m}'$. Now the projection mappings of the direct sum $\mathfrak{m} \oplus \mathfrak{m}'$ onto $\mathfrak{m}$ and $\mathfrak{m}'$ can be given by the right multiplication of elements e and e' of A^* respectively. Consider the right annihilator $r(\mathfrak{m})$ of $\mathfrak{m}$ in A^*, which evidently contains $\mathfrak{r}$. Then e is not in $r(\mathfrak{m})$ but e' is in $r(\mathfrak{m})$. Hence we have $r(\mathfrak{m}) = \mathfrak{r}$ (because $\mathfrak{r}$ is maximal), so that e' is in $\mathfrak{r}$. But since $\mathfrak{m}' \subseteq l_Q(\mathfrak{r})$, it follows necessarily that $\mathfrak{m}'e' = 0$, and this is a contradiction. Thus it is proved that Q is quasi-Frobenius.

As an immediate specialization of Proposition 3, we have easily

Theorem 2. *Let Q be a faithful two-sided A-A^*-module, and suppose that Q is completely reducible with respect to A. Then Q is quasi-Frobenius if and only if A^* is a dense subring*[5] *of the A-endomorphism ring of Q.*[6]

[5] Generally, a subring D of the endomorphism ring of an A-module Q is said to be dense if for any given finite number of elements $u_1, u_2, \cdots, u_n$ of Q and any given endomorphism f of Q, there exists an element d in D such that $u_1 d = u_1 f, u_2 d = u_2 f, \cdots, u_n d = u_n f$. Cf. [7].

[6] In view of this and Theorem 1, we can immediately deduce that if a faithful two-

Next, we proceed to the following

THEOREM 3. *Let Q be a faithful two-sided A-A^*-module, and suppose that Q is weakly distinguished with respect to A and every A-homomorphism of any finitely generated A-submodule of Q into the A-socle of Q can be given by the right multiplication of an element of A^*. Then Q is quasi-Frobenius.*

Proof. Consider a non-zero element u of Q, and denote by $l(u)$ the left annihilator of u in A. Associating the coset of any $a \in A$ modulo $l(u)$ with the element au, $A - l(u)$ is mapped isomorphically onto the cyclic A-submodule Au of Q. Since $l(u) \neq A$, there exists a maximal left ideal $\mathfrak{I}$ of A containing $l(u)$. Then evidently $Au - \mathfrak{I}u \cong A - \mathfrak{I}$, and therefore Q must, since it is weakly distinguished, contain an irreducible A-submodule isomorphic to $A - \mathfrak{I}$, that is, $r_Q(\mathfrak{I}) \neq 0$. Take any non-zero element v from $r_Q(\mathfrak{I})$. Then the mapping $au \rightarrow av$, $a \in A$, is obviously an A-homomorphism of Au onto the irreducible A-submodule Av, and hence there exists an element a^* of A^* such that $ua^* = v$. Thus we have shown that $uA^* \supseteq r_Q(\mathfrak{I})$. This implies in particular that every irreducible A^*-submodule of Q is of the form $r_Q(\mathfrak{I})$ with a suitable maximal left ideal $\mathfrak{I}$ of A (and conversely, any non-zero annihilator of such form is A^*-irreducible). Consequently, the A^*-socle of Q is contained in (and in fact coincides with) the A-socle of Q. Our theorem now follows immediately from Proposition 3.

Now we have the following main theorem:

THEOREM 4. *Let Q be an injective and distinguished left A-module, and let A^* be a dense subring of the A-endomorphism ring of Q. Then Q is quasi-Frobenius, when regarded as a two-sided A-A^*-module.*

Proof. By virtue of Theorem 3, we have only to prove that Q is faithful with respect to A. Let c be any non-zero element of A. Then the left annihilator $l(c)$ of c in A is a proper left ideal, and therefore $r_Q(l(c)) \neq 0$. Take now a non-zero element u from $r_Q(l(c))$. Then the mapping $ac \rightarrow au$,

---

sided A-A^*-module Q is completely reducible with respect to A and if A^* is dense in the A-endomorphism ring of Q, then Q is also completely reducible with respect to A^* and A is dense in the A^*-endomorphism ring of Q, and conversely; moreover, in this case, homogeneous A-components and A^*-components of Q coincide. This fact, however, remains true even when A and A^* do not possess identity elements, as can easily be seen from the later remark at the end of this section, and therefore we have obtained Jacobson [7, Theorems VI. 1. 1 and VI. 2. 1]. Indeed, our proof of Proposition 3 may be seen, partly, as a modification of the proof of the former theorem.

$a \in A$, is an A-homomorphism of Ac into Q. Hence there exists, due to the injectivity of Q, an element v in Q such that $cv = u$, which shows that $cQ \neq 0$.

We shall next show that, under certain chain conditions, the converse of Theorems 3 and 4 is also true:

THEOREM 5. *Let Q be a quasi-Frobenius two-sided A-A^*-module. Then A satisfies the left minimum condition if and only if Q satisfies both the maximum and the minimum conditions for A^*-submodules. And, if this is the case,* (1) *A coincides with the A^*-endomorphism ring of Q,* (2) *Q is both injective and distinguished with respect to A,* (3) *A^* is a dense subring of the A-endomorphism ring of Q,*[7] (4) *every A^*-homomorphism of any A^*-submodule of Q into Q can be extended to an A^*-endomorphism of Q,* (5) *Q is weakly distinguished with respect to A^*.*

Proof. Since Q is faithful with respect to A, the left A-module A and the right A^*-module Q form an orthogonal pair (with respect to Q). If we apply Proposition 2 to this orthogonal pair, we get immediately the first assertion and (1). Apply next, assuming the chain conditions, the Corollary of Proposition 2 to the same orthogonal pair. Then, firstly, we know that, for every left ideal $\mathfrak{l}$ of A, $l_A(r_Q(\mathfrak{l})) = \mathfrak{l}$ holds and moreover $Q - r_Q(\mathfrak{l})$ is regarded as the right-dual module of $\mathfrak{l}$. The former fact implies that $r_Q(\mathfrak{l}) \neq 0$ whenever $\mathfrak{l} \neq A$, that is, Q is distinguished, while the latter fact means that every A-homomorphism of any $\mathfrak{l}$ into Q can be obtained by the right multiplication of an element of Q, that is, Q is A-injective. Secondly, we can see that, for any A^*-submodule R of Q, the factor module $A - l(R)$ modulo the left annihilator $l(R)$ of R in A may be regarded as the left-dual module of R, which means, in view of (1), nothing but (4). Let now L be a finitely generated A-submodule of Q, and denote by $r(L)$ the right annihilator of L in A^*. Then L satisfies both the maximum and the minimum conditions for A-submodules, and L and $A^* - r(L)$ form an orthonal pair. Hence, Proposition 2 can again be applied to conclude that every A-homomorphism of L into Q may be given by the right multiplication of an element of A^*, and this implies, in particular, (3). To show finally that Q is weakly A^*-distinguished, consider two A^*-submodules R and R' of Q such that $R \supset R'$ and $R - R'$ is A^*-irreducible. Then it follows again from the Corollary of Proposition 2 that $l(R) \neq l(R')$, and so we can find an element a in $l(R')$ which is not in $l(R)$. The left multiplication of a evidently maps

[7] This fact may be regarded as an extension of the density theorem for irreducible modules (cf. [7, p. 31]).

$R-R'$ isomorphically onto an irreducible A^*-submodule of Q. This completes the proof of our theorem.

By combining Theorem 4 with Theorem 5 (and by symmetry), we have the following special case:

THEOREM 6. *Let A and A^* be two rings, and let Q be a two-sided A-A^*-module. Then the following conditions are equivalent:*

(i) *A satisfies the left minimum condition, Q is injective, distinguished and finitely generated with respect to A, and A^* coincides with the A-endomorphism ring of Q.*[8]

(ii) *A^* satisfies the right minimum condition, Q is injective, distinguished and finitely generated with respect to A^*, and A coincides with the A^*-endomorphism ring of Q.*

(iii) *Q is quasi-Frobenius, and A and A^* satisfy, respectively, the left and the right minimum conditions.*

(iv) *Q is quasi-Frobenius, A satisfies the left minimum condition, and Q is finitely generated with respect to A.*

(v) *Q is quasi-Frobenius, A^* satisfies the right minimum condition, and Q is finitely generated with respect to A^*.*

We now turn to the general case. Let Q be a quasi-Frobenius two-sided A-A^*-module. Let M be an irreducible left A-module such that Q contains an isomorphic image of it, or equivalently, the right-dual module M^* of M is irreducible. Then M may be regarded as the left-dual module of M^* and moreover the homogeneous component of the socle of Q belonging to M coincides with the homogeneous component belonging to M^* (Theorem 1). Let Δ be the endomorphism division ring of M. Then [7, Theorem V. 7. 1], together with Proposition 3, implies that there is a lattice isomorphism between the lattice of A^*-submodules of the common homogeneous component and the lattice of Δ-submodules of M, and, in particular, the A^*-dimension of the homogeneous component coincides with the Δ-dimension of M. Thus we have

PROPOSITION 4. *Under the same assumptions as in Theorem 1, the A-*

---

[8] Here, the injectivity and the distinguishedness for Q may, by virtue of Theorem 3, be replaced respectively by the weaker conditions that every A-homomorphism of any A-submodule of Q into Q can be extended to an A-endomorphism of Q and that Q is weakly distinguished with respect to A.

and the A^*-dimensions of the homogeneous component of the socle belonging to M, or to M^*, coincide with the capacites of M^* and M respectively.

Now, we call a quasi-Frobenius Q *Frobenius* if, for any irreducible left A-module M such that Q contains an isomorphic image of it, the capacity of M coincides with that of the right-dual M^* of M, or what defines the same thing, if the A- and the A^*-dimensions of each homogeneous component of the socle of Q coincide.

The following proposition is not only for quasi-Frobenius modules but also for Frobenius modules and may be verified quite easily:

PROPOSITION 5. *Let Q be a quasi-Frobenius (or Frobenius) two-sided A-A^*-module and let Q_0 be an A-A^*-submodule of Q. Then $\mathfrak{z}=l_A(Q_0)$ and $\mathfrak{z}^*=r_{A^*}(Q_0)$ are two-sided ideals of A and A^* respectively, and Q_0 is quasi-Frobenius (or Frobenius) when regarded as a two-sided $A/\mathfrak{z}—A^*/\mathfrak{z}^*$-module.*

Assume again the left and the right minimum conditions for A and A^* respectively. Then left ideals $\mathfrak{l}$ of A and A^*-modules R of (the quasi-Frobenius module) Q correspond one-to-one by the annihilator relations (Corollary of Proposition 2), and it is evident that $\mathfrak{l}$ is a two-sided ideal if and only if the corresponding R is an A-A^*-submodule; the similar is also the case for right ideals of A^* and A-submodules of Q. This, together with Proposition 5, yields

THEOREM 7. *Let A and A^* satisfy the left and the right minimum conditions respectively, and let Q be a quasi-Frobenius (or Frobenius) two-sided A-A^*-module. Then there is a one-to-one correspondence between two-sided ideals $\mathfrak{z}$ of A, A-A^*-submodules Q_0 of Q, and two-sided ideals $\mathfrak{z}^*$ of A^* by the annihilator relations:*

$$r_Q(\mathfrak{z})=Q_0, \qquad \mathfrak{z}=l_A(Q_0),$$
$$r_{A^*}(Q_0)=\mathfrak{z}^*, \qquad Q_0=l_Q(\mathfrak{z}^*);$$

and, in this case, Q_0 is quasi-Frobenius (or Frobenius) when regarded as a two-sided $A/\mathfrak{z}$-$A^*/\mathfrak{z}^*$-module.

Example. Let A be a ring without non-zero nilpotent ideals. Then it is quasi-Frobenius when regarded as a two-sided A-module. To prove this, consider an irreducible left ideal $\mathfrak{l}$ of A. Then it is generated by an idempotent element e ([7, Proposition III. 9. 1]) : $\mathfrak{l}=Ae$. One can now easily see that the right-dual module of $\mathfrak{l}$ with respect to A is isomorphic to eA, whereas the latter is an irreducible right ideal of A by virtue of [7, Corollary of Proposition IV. 3. 1]. Similarly, the left-dual module of every irreducible

right ideal of A is irreducible too, and this shows our assertion. It should be noted, in view of this, that [7, Theorem IV. 3. 1] may be interpreted as a special case of our Theorem 1.

Suppose next that A is a ring whose left socle S is faithful. Then A is semi-simple, and, in particular, it has no non-zero nilpotent ideals. Hence, it follows (from either of the above mentioned theorems) that S coincides with the right socle of A. Let $\mathfrak{z}$ be a non-zero two-sided ideal of A. Then $\mathfrak{z}S \neq 0$, and so there is an irreducible left ideal $\mathfrak{l}$ such that $\mathfrak{z}\mathfrak{l} \neq 0$, whence $\mathfrak{z}\mathfrak{l} = \mathfrak{l}$. But this implies $S\mathfrak{z} \neq 0$, because $S\mathfrak{z}\mathfrak{l} = S\mathfrak{l} \supseteq \mathfrak{l}^2 \neq 0$. Thus it is shown that S is a faithful right ideal of A, and we know from Proposition 5 that *if A is a ring having a faithful completely reducible left ideal, then* (*not only A but also*) *the common socle of A is quasi-Frobenius when regarded as a two-sided A-module.*

Remark. The notion of quasi-Frobenius two-sided A-A^*-modules Q may be transferred to the case when A and A^* do not necessarily have identity elements but Q satisfies $r_Q(A) = 0$ and $l_Q(A^*) = 0$, by taking the conditions i) and ii) as its definition, provided we restrict, in ii), both maximal left and maximal right ideals $\mathfrak{l}$ and $\mathfrak{r}$ to be modular (cf. [7, p. 5]). It is then almost evident that we may also replace ii) in this definition by the condition ii′). Furthermore, if we observe that the results stated in § 1, except those which are concerned with injectivity, remain valid for modular left ideals $\mathfrak{l}$ when A does not have an identity element but Q satisfies $r_Q(A) = 0$, we can examine, without difficulties, that all the propositions and the theorems in § 2, including the above example, still hold in our case under obvious additional assumptions, provided we require the existence of identity elements only for A in Theorem 4 as well as for A and A^* in (i) and (ii) of Theorem 6. For instance, we have to asume additionally that in Theorem 3, each element u of Q is always in Au, while in Theorem 5, A satisfies the left maximum condition. It is however to be noted that Theorem 2 remains true even without assuming that $r_Q(A) = 0$ and $l_Q(A^*) = 0$, because these conditions follow automatically from the complete reducibility for Q and the denseness of A^* respectively.

3. Duality theorems.

LEMMA 1. *Let Q be an injective left A-module and A^* its A-endomorphism ring. Let M be a left A-module and M^* its right-dual module with respect to Q. Then, for any $x \in M$ and $f \in M^*$, we have*

$$r_Q(l_A(x)) = xM^*, \qquad r(l(f)) = fA^*,$$

where $r(\ )$ and $l(\ )$ in the second equality mean the right and the left annihilators in M^* and M respectively.

Proof. Let u be an element in $r_Q(l_A(x))$. Then the mapping $ax \to au$, $a \in A$, is an A-homomorphism of Ax into Q, and it can, since Q is A-injective, be extended to an A-homomorphism $g(\in M^*)$ of M into $Q: xg = u$. This shows that $r_Q(l_A(x)) \subseteq$ whence $= xM^*$. Similarly, if h is an element in $r(l(f))$ the A-homomorphism $xf \to xh$, $x \in M$, can be extended to an A-endomorphism $a^*(\in A^*)$ of $Q: fa^* = h$, which shows $r(l(f)) = fA^*$.

PROPOSITION 6. *Under the same assumptions as in Lemma 1, suppose in addition that Q is A-distinguished. Then $x = 0$ is the only element of M such that $xM^* = 0$. More generally, we have $l(r(L)) = L$ for every A-submodule L of M.*

Proof. Let x be a non-zero element of M. Then $xM^* = r_Q(l_A(x))$ by Lemma 1, while the right side is non-zero because $l_A(x)$ is a proper left ideal of A and Q is distinguished. The second assertion may immediately be seen by applying this first one to the left A-module $M - L$ and its right-dual module $r(L)$.

We now get the following

THEOREM 8. *Let A and A^* be two rings satisfying the left and the right minimum conditions respectively and let Q be a quasi-Frobenius two-sided A-A^*-module. (Or equivalently, let A, A^* and Q satisfy one of the equivalent conditions in Theorem 6.) Let M be a finitely generated left A-module and let M^* be its right-dual module with respect to Q. Then M^* is also finitely generated (with respect to A^*) and M coincides with the left-dual module of M^*. The same holds also for every finitely generated right A^*-module.*

Proof. Since Q is both A-injective and A-distinguished, M and M^* form an orthogonal pair with respect to Q according to Proposition 6. On the other hand, the finitely generated left A-module M satisfies, because of the left minimum condition for A, both the maximum and the minimum conditions for A-submodules. Our theorem now follows immediately from Proposition 2.

We shall next prove the following converse of Theorem 8:

THEOREM 9. *Let Q be a two-sided A-A^*-module. Suppose that, for each finitely generated left A-module M, the right-dual module M^* is also*

finitely generated and moreover M coincides with the left-dual module of M^*, and suppose that the same holds for each finitely generated right A^*-module. Then A and A^* satisfy the left and the right minimum conditions respectively and moreover Q is quasi-Frobenius.

Proof. Consider a finitely generated left A-module M and its right-dual module M^*. Let L be an A-submodule of M. Then the right annihilator $r(L)$ of L in M^* may be regarded as the right-dual module of $M-L$. Since $M-L$ is finitely generated, $r(L)$ is also finitely generated and moreover $l(r(L))=L$, according to our assumptions. Similarly, we know that, for each A^*-submodule R of M^*, the left annihilator $l(R)$ is finitely generated and moreover $r(l(R))=R$. These together show that A-submodules L of M and A^*-submodules R of M^* are all finitely generated and L and R correspond one-to-one by the annihilator relations. However, the former fact means, as is well-known, that M and M^* satisfy the maximum condition for A- and A^*-submodules respectively, and this, together with the latter fact, yields that M and M^* fulfill also the minimum condition. Now, we take in particular $M=A_s$ whence $M^*=Q$. Then it follows that A satisfies the left minimum condition, $l_A(Q)=0$, i.e., Q is A-faithful, and $r_Q(\mathfrak{l})$ is A^*-irreducible for every maximal left ideal $\mathfrak{l}$ of A. Furthermore, the similar must, by symmetry, be the case for A^* and the A-module Q, and this shows that Q is quasi-Frobenius.

Now suppose that M_1 and M_2 are two left (or right) A-modules. For any A-homomorphism $\phi\colon M_1\rightarrow M_2$ and any element $x\in M_1$, we denote by $x\phi$ (or ϕx) the image of x by ϕ. If further ψ is an A-homomorphism of M_2 into a third left (or right) A-module M_3, we shall denote by $\phi\circ\psi$ (or $\psi\circ\phi$) the composite mapping $x\rightarrow(x\phi)\psi$ (or $x\rightarrow\psi(\phi x)$). Let Q be a two-sided A-A^*-module, and let $M_1{}^*$ and $M_2{}^*$ be the right-dual modules of M_1 and M_2 respectively. Then we can associate with each ϕ an A^*-homomorphism $\phi^*\colon M_2\rightarrow M_1{}^*$ by setting $\phi^*g=\phi\circ g$, $g\in M_2{}^*$, i.e.,

$$(*)\qquad x(\phi^*g)=(x\phi)g,\qquad x\in M_1, g\in M_2{}^*.$$

ϕ^* is called the *dual mapping* of ϕ with respect to Q, and it satisfies, with any A-homomorphism $\psi\colon M_2\rightarrow M_3$, $(\phi\circ\psi)^*=\phi^*\circ\psi^*$. Thus, the association $M^*\rightarrow M^*$, together with the mapping $\phi\rightarrow\phi^*$, defines a contravariant functor of one variable in the sense of [1]. Suppose now that A and A^* satisfy, respectively, the left and the right minimum conditions and Q is quasi-Frobenius. Suppose in addition that both M_1 and M_2 are finitely generated. Then M_1 and M_2 may, by Theorem 8, be looked upon as the left-dual modules of $M_1{}^*$ and $M_2{}^*$ respectively, and therefore the above equality $(*)$ shows that

ϕ coincides with the dual mapping of ϕ^*. Thus, the mapping $\phi \rightarrow \phi^*$ gives an isomorphism between two groups $\mathrm{Hom}_A(M_1, M_2)$ and $\mathrm{Hom}_{A^*}(M_2^*, M_1^*)$. Moreover, it follows from Theorem 8 that the M^*'s exhaust, up to isomorphisms, all finitely generated right A^*-modules when M runs over all finitely generated left A-modules. We can however prove a complete converse of these situations:

THEOREM 10. *Let A and A^* be two rings. Suppose that we have a contravariant functor T (of one variable), defined only for finitely generated left A-modules M and taking finitely generated right A^*-modules as its values $T(M)$, such that the $T(M)$'s, up to isomorphisms, cover all finitely generated right A^*-modules and moreover T maps* $\mathrm{Hom}_A(M_1, M_2)$ *isomorphically onto* $\mathrm{Hom}_{A^*}(T(M_2), T(M_1))$ *for any finitely generated left A-modules M_1 and M_2. Then A and A^* satisfy the left and the right minimum conditions respectively, and there exists in fact a quasi-Frobenius two-sided A-A^*-module Q such that T is naturally equivalent*[9] *with the functor which is defined by associating every finitely generated left A-module M with its right-dual module M^* with respect to Q.*

Proof. There exists a finitely generated left A-module Q such that $T(Q)$ is isomorphic to the right A^*-module A^*. We may however assume, without loss of generality, that $T(Q) = A^*$. The left multiplication of an element a^* of A^* induces on A^* an A^*-endomorphism, and there must be a unique A-endomorphism of Q which is mapped by T onto it. If we identify this with a^*, Q can, since T is contravariant, be converted into a two-sided A-A^*-module. Consider a finitely generated left A-module M and its right-dual module $M^* = \mathrm{Hom}_A(M, Q)$. Then the mapping $f \rightarrow T(f)$, $f \in M^*$, is an isomorphism of M^* onto $\mathrm{Hom}_{A^*}(A^*, T(M))$, whereas the latter module may be identified naturally with $T(M)$.[10] Moreover, the above mapping is actually an A^*-isomorphism, because $T(fa^*) = (T(f \circ a^*) =) T(f) \circ T(a^*)$ should be identified with the element $T(f)a^*$ of $T(M)$. Now let M_1 and M_2 be two finitely generated left A-modules. Let ϕ be an A-homomorphism of M_1 into M_2 and ϕ^*: $M_2^* \rightarrow M_1^*$ its dual mapping. Then $T(\phi^* g) = T(\phi \circ g) = T(\phi) \circ T(g)$ for any $g \in M_2^*$, and the last term is, when $T(g)$ is regarded as an element of $T(M_2)$, identified with $T(\phi)T(g)$, i.e., we have the commutativity of the following diagram:

[9] Cf. [1, p. 20].

[10] That is, we identify each element of $T(M)$ with the multiplication effected by it in A^*; the element is conversely characterized as the image of the identity element of A^* by the identified A^*-homomorphism.

$$\begin{array}{ccc} M_2^* & \xrightarrow{T} & T(M_2) \\ \phi^* \downarrow & & \downarrow T(\phi) \\ M_1^* & \xrightarrow{T} & T(M_1). \end{array}$$

Thus it is shown that T yields a natural equivalence between two functors $M \to M^*$ and T.

In order to prove the remaining part of our theorem, we may evidently assume that both functors coincide. Let M be a finitely generated left A-module, as above, and consider an A^*-homomorphism ξ of the right-dual module $T(M)$ of M into Q. Since Q is identified with the right-dual module $T(A)$ of A_s, there exists a unique A-homomorphism ϕ of A_s into M such that the dual mapping $T(\phi): f \to \phi \circ f$, $f \in M^*$, coincides with ξ. If x is an element of M which is identified with ϕ, then xf may also be identified with $\phi \circ f$ and so we have $xf = \xi f$ (for all $f \in M^*$). Thus it is shown that M coincides with the left-dual module of $T(M)$. Since moreover the $T(M)$'s range, up to isomorphisms, over all finitely generated right A^*-modules, it follows from Theorem 9 that A and A^* satisfy the left and the right minimum conditions respectively and Q is quasi-Frobenius.

Remark. Lemma 1 may be regarded as an extension of the first part of Ikeda and Nakayama [6, Theorem 1]. And by making use of Lemma 1, we can easily generalize the last part of this theorem in the following form: *under the same assumptions as in Lemma* 1, $r(L_1 \cap L_2) = r(L_1) + r(L_2)$ *for any A-submodules L_1 and L_2 of M, and $r(l(R)) = R$ for all finitely generated A^*-submodules R of M^*.* As an immediate consequence of this, we know that if M satisfies the minimum condition for A-submodules, then M^* satisfies the maximum condition for A^*-submodules, and moreover if M satisfies both the maximum and the minimum conditions for A-submodules, then so does M^* for A^*-submodules. In particular, if A satisfies the left minimum condition, then Q satisfies both the maximum and the minimum conditions for A^*-submodules, while if Q satisfies both the maximum and the minimum conditions for A-submodules, then A^* satisfies the right minimum condition.

4. Injective modules and quasi-Frobenius rings. Let A be a ring, and let M be a left A-module. An extension A-module M' of M is called an *essential extension* of M if $M'' = 0$ is the only A-submodule of M' such that $M'' \cap M = 0$. After showing that injective modules may be characterized as those modules which have no essential extensions other than themselves,

Eckmann and Schopf [2] proved the existence and the uniqueness (up to isomorphisms over M) of an injective essential extension $\hat{M}$ of any given (left A-module) M. Moreover, every injective extension of M contains such an $\hat{M}$, and therefore injective essential extensions are nothing but minimal injective extensions.

PROPOSITION 7. *An injective left A-module $Q\,(\neq 0)$ is directly indecomposable if and only if it is an essential extensions of every non-zero A-submodule.*

Proof. Suppose that Q is directly indecomposable. Let M be a non-zero A-submodule. Then Q contains an injective essential extension $\hat{M}$ of M. Since $\hat{M}$ is a direct summand of Q, we must have $Q = \hat{M}$. Suppose, conversely, Q is directly decomposable into two non-zero A-submodules, say, M and M': $Q = M \oplus M'$. Then necessarily $M \cap M' = 0$, which shows that Q is not an essential extension of M.

COROLLARY. *Let Q be an injective left A-module containing an irreducible A-submodule M. Then the following conditions are equivalent:*

(i) *Q is directly indecomposable.*

(ii) *M is a smallest A-submodule*[11] *of Q.*

(iii) *Q is an essential extension of M.*

Proof. The implication (i) $\Rightarrow$ (iii) is the special case of the preceding proposition, while the implications (iii) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i) hold evidently without the assumption of injectivity for Q.

PROPOSITION 8. *If A satisfies the left maximum condition, a direct sum of left A-modules is injective if and only if so is each direct summand.*[12]

Proof. The "only if" is well-known and is easy to see. So we have only to prove the "if" part. Suppose that a left A-module Q is a direct sum of injective A-submodules Q_μ: $Q = \sum_\mu \oplus Q_\mu$, and denote by ϵ_μ the projection mapping of Q onto Q_μ for each μ. Let $\mathfrak{l}$ be a left ideal of A, and suppose that there is given an A-homomorphism $\phi: \mathfrak{l} \to Q$. Then there exists, since the composite mapping $\phi \circ \epsilon_\mu$ is an A-homomorphism of $\mathfrak{l}$ into Q_μ, an element u_μ in Q_μ such that $(a\phi)\epsilon_\mu = (a(\phi \circ \epsilon_\mu) =) au_\mu$ for all $a \in \mathfrak{l}$; here,

[11] By a smallest A-submodule we mean a non-zero A-submodule which is contained in all non-zero A-submodules; it is of course the only minimal A-submodule, if it exists.

[12] Cf. [1, Exercise I. 8].

we may of course take $u_\mu = 0$ whenever $(\mathfrak{l}\phi)\epsilon_\mu = 0$. But since A satisfies the left maximum condition, $\mathfrak{l}$ and hence $\mathfrak{l}\phi$ is finitely generated, so that $(\mathfrak{l}\phi)\epsilon_\mu = 0$, or $u_\mu = 0$ except for only a finite number of μ. Now their sum $u = \sum_\mu u_\mu$ fulfills $au = a\phi$ for all $a \in \mathfrak{l}$, and this shows the injectivity of Q.

Suppose, from now on, that A satisfies the left minimum condition. Let N be the radical of A, and let $\bar{A}$ denote the (semi-simple) factor ring A/N, or the factor module $A - N$. Then $\bar{A}$ is a direct sum sum of orthogonal simple subrings $\bar{A}_1, \bar{A}_2, \cdots, \bar{A}_k$. Let $\bar{e}_\kappa$ be, for each κ, a primitive idempotent element in $\bar{A}_\kappa$. Then $\bar{e}_\kappa \bar{A} \bar{e}_\kappa$ is a division ring, and $\bar{A}_\kappa$ is (ring-)isomorphic with the total matric algebra over $\bar{e}_\kappa \bar{A} \bar{e}_\kappa$ of a finite degree $f(\kappa)$. In fact, $\bar{A}\bar{e}_\kappa$ is an irreducible left $\bar{A}$- or A-module whose endomorphism ring is $\bar{e}_\kappa \bar{A} \bar{e}_\kappa$ and whose capacity is $f(\kappa) : [\bar{A}\bar{e}_\kappa : \bar{e}_\kappa \bar{A} \bar{e}_\kappa] = f(\kappa)$, and $\bar{A}_\kappa$ is, as left A-module, isomorphic to the $f(\kappa)$-times direct sum of $\bar{A}\bar{e}_\kappa$: $\bar{A}_\kappa \cong (\bar{A}\bar{e}_\kappa)^{f(\kappa)}$. Moreover, the k modules $\bar{A}\bar{e}_1, \bar{A}\bar{e}_2, \cdots, \bar{A}\bar{e}_k$ exhaust, up to isomorphisms, all irreducible left A-modules. There exists, for each κ, an idempotent representative $e_\kappa (\in A)$ of the coset $\bar{e}_\kappa$. The k idempotent elements $e_1, e_2, \cdots, e_k$ are all primitive and non-isomorphic, and any primitive idempotent element of A is isomorphic to one of them. Furthermore, A is, as left A-module, isomorphic to the direct sum $\sum_{\kappa=1}^{k} \oplus (Ae_\kappa)^{f(\kappa)}$; the isomorphism naturally yields a decomposition of the identity element 1 of A into orthogonal primitive elements $e_{\kappa i}$, $\kappa = 1, 2, \cdots, k$, $i = 1, 2, \cdots, f(\kappa)$, such that $e_{\kappa i}$ is, for each κ, isomorphic to e_κ and $A = \sum_{\kappa=1}^{k} \oplus \sum_{i=1}^{f(\kappa)} \oplus Ae_{\kappa i}$ gives a direct decomposition of A into directly indecomposable left ideals.

Now, we denote by Q_κ the minimal injective extension of the irreducible left-A-module $\bar{A}\bar{e}_\kappa$. Then, according to the Corollary of Proposition 7, Q_κ is directly indecomposable and has $\bar{A}\bar{e}_\kappa$ as a smallest A-submodule, and conversely any directly indecomposable injective left A-module is isomorphic with some Q_κ. Consider a left A-module Q. Then the right annihilator $r_Q(N)$ of the radical N is, as is well-known, the socle of Q, and moreover Q is its essential extension. Suppose now $r_Q(N) \cong \sum_{\kappa=1}^{k} \oplus (\bar{A}\bar{e}_\kappa)^{g(\kappa)}$ with non-negative cardinal numbers $g(\kappa)$, and consider the direct sum $Q' = \sum_{\kappa=1}^{k} \oplus (Q_\kappa)^{g(\kappa)}$. Then Q' is injective by virtue of Proposition 8, and therefore the above isomorphism of $r_Q(N)$ onto $\sum_{\kappa=1}^{k} \oplus (\bar{A}\bar{e}_\kappa)^{g(\kappa)}$ can be extended to an isomorphism of Q into Q' ([2, 4. i. 2]). Since, however, $\sum_{\kappa=1}^{k} \oplus (\bar{A}\bar{e})_\kappa{}^{g(\kappa)}$ is the socle of Q',

Q' is necessarily an essential extension of the isomorphic image of Q. From this follows immediately the following generalization of Nagao and Nakayama [10, Theorem 2]:

THEOREM 11. *A left module of a ring A satisfying the left minimum condition is injective if and only if it is a (finite or infinite) direct sum of A-submodules each of which is isomorphic to some Q_κ, where Q_κ is the minimal injective extension of an irreducible left A-module $\bar{A}\bar{e}_\kappa$ which is the homomorphic image of a directly indecomposable left component Ae_κ of A.*

Let Q be an injective left A-module, i. e., $Q \cong \sum_{\kappa=1}^{k} \oplus (Q_\kappa)^{g(\kappa)}$, with uniquely determined multiplicities $g(\kappa)$. It is then evident that Q is distinguished if and only if $g(\kappa) \neq 0$ for all κ, and Q is, in this case, finitely generated if and only if all Q_κ are finitely generated and all $g(\kappa)$ are finite. Suppose now that this is the case, that is, Q is both distinguished and finitely generated. Let A^* be the A-endomorphism ring of Q. Then A^* satisfies the right minimum condition by Theorem 6, and there exist in A^* a complete system of non-isomorphic primitive idempotents $e_1^*, e_2^*, \cdots, e_k^*$ (just like $e_1, e_2, \cdots, e_k$ in A) such that $Qe_\kappa^* \cong Q_\kappa$ for each κ. On the other hand, consider an A^*-module $e_\kappa Q$, which is a direct summand of the right A^*-module Q. Since Q is also A^*-injective and A coincides with its A^*-endomorphism ring again by Theorem 6, $e_\kappa Q$ is necessarily both injective and directly indecomposable, and therefore it contains, according to the Corollary of Projosition 7, a smallest A^*-submodule. These facts show the necessity of the following theorem:

THEOREM 12. *Let A and A^* be two rings satisfying the left and the right minimum conditions respectively and let $e_1, e_2, \cdots, e_k$ be a complete system of non-isomorphic primitive idempotent elements in A. Let Q be a faithful two-sided A-A^*-module. In order that Q be quasi-Frobenius it is necessary and sufficient that A^* have exactly k non-isomorphic primitive idempotent elements $e_1^*, e_2^*, \cdots, e_k^*$ and they, if suitably ordered, satisfy the following conditions:*

i) *the left A-module Qe_κ^* contains, for each κ, a smallest A-submodule and this is isomorphic to $\bar{A}\bar{e}_\kappa$, the homomorphic image of Ae_κ modulo the radical of A.*

ii) *the right A^*-module $e_\kappa Q$ contains, for each κ, a smallest A^*-submodule.*

And, if this is the case, the smallest A^*-submodule of $e_\kappa Q$ is isomorphic to $\bar{e}_\kappa^* \bar{A}^*$, the homomorphic image of $e_\kappa^* A^*$ modulo the radical of A^*.

The sufficiency can, however, be proved in the similar way as in (the first half of) the proof of Nakayama [12, Theorem 6]. Namely, let $e_{\kappa i}^*$, $\kappa = 1, 2, \cdots, k$, $i = 1, 2, \cdots, g(\kappa)$, denote similar orthogonal primitive idempotent elements in A^* as $e_{\kappa i}$ in A: $e_{\kappa i}^* \cong e_\kappa^*$, $1 = \sum_{\kappa=1}^{k} \sum_{i=1}^{g(\kappa)} e_{\kappa i}^*$. In view of the fact that $r_Q(N)$ is an A-A^*-submodule of Q, we have then the direct decomposition $r_Q(N) = \sum_{\kappa=1}^{k} \oplus \sum_{i=1}^{g(\kappa)} \oplus\, r_Q(N) e_{\kappa i}^*$, where $r_Q(N) e_{\kappa i}^* \cong r_Q(N) e_\kappa^*$ (as left A-modules). But since $r_Q(N)$ is the A-socle of Q, $r_Q(N) e_\kappa^* = r_Q(N) \cap Q e_\kappa^*$ is by virtue of the assumption i), necessarily the smallest A-submodule of $Q e_\kappa^*$ and is isomorphic to $\bar{A}\bar{e}_\kappa$. This implies that each $\sum_{i=1}^{g(\kappa)} \oplus\, r_Q(N) e_{\kappa i}^*$ is a homogeneous (A-)component of $r_Q(N)$, and hence is an A-A^*-submodule. Moreover, it is a minimal A-A^*-submodule. For, if u is any non-zero element in it then $u e_{\kappa p}^* \neq 0$ for some p; but $A u e_{\kappa p}^* = r_Q(N) e_{\kappa p}^*$, because of the irreducibility of the right side, and therefore

$$A u A^* \supseteq A u e_{\kappa p}^* A^* = r_Q(N) e_{\kappa p}^* A^* \supseteq \sum_{i=1}^{g(\kappa)} \oplus\, r_Q(N) e_{\kappa i}^*.$$

Let now N^* be the radical of A^*. Then every minimal two-sided A-A^*-module is, since N^* is nilpotent, annihilated by N^*, and, in particular, we have $\sum_{i=1}^{g(\kappa)} \oplus\, r_Q(N) e_{\kappa i}^* \subseteq l_Q(N^*)$. Since this is true for every κ, it follows that $r_Q(N) \subseteq l_Q(N^*)$. Now, $l_Q(N^*)$ is the A^*-socle of Q and hence $e_\kappa l_Q(N^*) = l_Q(N^*) \cap e_\kappa Q$ is, by the assumption ii), the smallest A^*-submodule of $e_\kappa Q$. But since $e_\kappa r_Q(N) e_\kappa^* \subseteq e_\kappa l_Q(N^*) e_\kappa^*$ and $e_\kappa r_Q(N) e_\kappa^* \neq 0$ (because $r_Q(N) e_\kappa^* \cong \bar{A}\bar{e}_\kappa$), we have $e_\kappa l_Q(N^*) e_\kappa^* \neq 0$, whence $e_\kappa l_Q(N^*) \cong \bar{e}_\kappa^* \bar{A}^*$. From this and by symmetry, we can conclude that $r_Q(N)$ ($\supseteq$ whence) $= l_Q(N^*)$; observe that we have derived the above relation $r_Q(N) \subseteq l_Q(N^*)$ from the condition i) only.

Consider now any irreducible left A-module $\bar{A}\bar{e}_\kappa$. It is isomorphic to the factor module $A - \mathfrak{l}$ modulo the maximal left ideal $\mathfrak{l} = A(1 - e_\kappa) + N$. Hence the right-dual module of $\bar{A}\bar{e}_\kappa$ with respect to Q is isomorphic to $r_Q(\mathfrak{l}) = r_Q(1 - e_\kappa) \cap r_Q(N) = e_\kappa Q \cap r_Q(N) = e_\kappa r_Q(N) = e_\kappa l_Q(N^*)$, which is A^*-irreducible as we have seen just above. Similarly, we may show that the left-dual module of every irreducible right A^*-module is A-irreducible too, and thus Q is quasi-Frobenius.

Now, Nakayama [12] called A, satisfying both the left and the right minimum conditions, to be a *quasi-Frobenius ring* if there exists a permutation $(\pi(1), \pi(2), \cdots, \pi(k))$ of $(1, 2, \cdots, k)$ such that for each κ,

i) $Ae_{\pi(\kappa)}$ contains a smallest left subideal and this is isomorphic to $\bar{A}\bar{e}_\kappa$,

ii) $e_\kappa A$ contains a smallest right subideal.

So, Theorem 12, combined with Theorem 6, yields the following

THEOREM 13. *A ring A satisfying the left minimum condition is a quasi-Frobenius ring if and only if it is quasi-Frobenius when regarded as a two-sided A-module.*

Owing to the preceding theorem, it follows from the Corollary of Proposition 2 in particular that *if A is a quasi-Frobenius ring, then $l(r(\mathfrak{l}))=\mathfrak{l}$ and $r(l(\mathfrak{r}))=\mathfrak{r}$ for every left ideal $\mathfrak{l}$ and right ideal $\mathfrak{r}$ of A.* Consider now a maximal right ideal $\mathfrak{r}$ of A such that $l(\mathfrak{r})\neq 0$. Let $\mathfrak{l}$ be an irreducible left subideal of $l(\mathfrak{r})$. Then $r(\mathfrak{l})=\mathfrak{r}$, because $r(\mathfrak{l})$ is clearly a proper right ideal containing $\mathfrak{r}$. From this and by symmetry, we can easily conclude that *if conversely $l(r(\mathfrak{l}))=\mathfrak{l}$ and $r(l(\mathfrak{r}))=\mathfrak{r}$ for every irreducible left ideal $\mathfrak{l}$ and irreducible right ideal $\mathfrak{r}$ of A, satisfying the left minimum condition, then A is quasi-Frobenius.*[13] Thus we have derived [12, Theorem 6]. Next, let n be a natural number and consider the direct sum A^n of n copies of A. A^n may be regarded as a left as well as a right A-module in the usual fashion, and it is evident that if we define the product of two vectors $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ to be $a_1b_1+a_2b_2+\cdots+a_nb_n$, the left A-module A^n and the right A-module A^n form an orthogonal pair with respect to A. Hence, we have, as a special case of the Corollary of Proposition 2, the following theorem of Hall [4]:[14] *If A is a quasi-Frobenius ring then $l(r(L))=L$ and $r(l(R))=R$ for every left A-submodule L and right A-submodule R of A^n.* On the other hand, Theorem 6 shows that a necessary and sufficient condition for A to be a quasi-Frobenius ring is that A be both injective and distinguished as left A-module. However, we may, for sufficient condition, omit the distinguishedness. To prove this, suppose that A is injective. Then each direct summand Ae_κ is also injective, so that it is, by (the Corollary of) Proposition 7, a minimal injective extension of its irreducible (in fact, smallest) left subideal $\mathfrak{l}_\kappa$. The k irreducible left ideals $\mathfrak{l}_1, \mathfrak{l}_2, \cdots, \mathfrak{l}_k$ are mutually non-isomorphic, since so are $Ae_1, Ae_2, \cdots, Ae_k$, and therefore they must coincide, up to isomorphisms and up to arrangements, with $\bar{A}\bar{e}_1, \bar{A}\bar{e}_2, \cdots, \bar{A}\bar{e}_k$. We thus obtain the following theorem of Ikeda [5] (cf. also [6], Eilenberg and Nakayama [3]): *A ring satisfying the left*

[13] We may here restrict further $\mathfrak{l}$ and $\mathfrak{r}$ to be nilpotent, because every non-nilpotent irreducible one-sided ideal is generated by an idempotent element and so satisfies the above annihilator relations.

[14] In [9], this was derived in just the same way. Cf. also [12, Theorem 12].

minimum condition is quasi-Frobenius if and only if is is left self-injective.

Now, consider again an injective left A-module $Q = \sum_{\kappa=1}^{k} \oplus (Q_\kappa)^{g(\kappa)}$; and suppose that Q is both finitely generated and distinguished, or what is the same thing, all Q_κ are finitely generated and all $g(\kappa)$ are non-zero and finite. Then the endomorphism ring A^* of Q satisfies the right minimum condition, and Q is quasi-Frobenius as two-sided A-A^*-module (Theorem 6); moreover, it is easy to see that, on retaining the notations in Theorem 12, the capacity of each irreducible right A^*-module $\bar{e}_\kappa^* \bar{A}^*$ is $g(\kappa)$. From this (and Theorem 6), we get immediately the following

THEOREM 14. *Let Q be a two-sided A-A^*-module, where A satsifies the left minimum condition. Then in order that Q be Frobenius and that A^* satisfy the right minimum condition it is necessary and sufficient that Q be, as left A-module, both isomorphic to $\sum_{\kappa=1}^{k} \oplus (Q_\kappa)^{f(\kappa)}$, the minimal injective extension of $\bar{A} = A - N$, and finitely generated and that moreover A^* be the A-endomorphism ring of Q.*

Nakayama [12] called A a *Frobenius ring* if it is quasi-Frobenius and moreover $f(\kappa) = f(\pi(\kappa))$ for every $\kappa = 1, 2, \cdots, k$. So we have, in particular,

THEOREM 15. *A ring A satisfying the left minimum condition is a Frobenius ring if and only if it is Frobenius when regarded as a two-sided A-module, that is, it is, as left A-module, isomorphic to the minimal injective extension of $\bar{A} = A - N$.*

As an application of Theorems 14 and 15, we prove the following

THEOREM 16.[15] *Let A be a Frobenius ring, and let $\mathfrak{z}$ be a two-sided ideal of A. Then the factor ring $A/\mathfrak{z}$ is Frobenius if and only if the right annihilator $r(\mathfrak{z})$ of $\mathfrak{z}$ is both left and right principal:*[16] $r(\mathfrak{z}) = Ac = cA$. *And, in this case, $A/\mathfrak{z}$ is isomorphic with $A/\mathfrak{z}^*$, where $\mathfrak{z}^*$ is the double right annihilator of $\mathfrak{z}$: $\mathfrak{z}^* = r(r(\mathfrak{z}))$.*

Proof. By Theorem 7, $r(\mathfrak{z})$ is Frobenius when regarded as a two-sided

[15] This is a generalization of [11, Theorem 9] and is also a modification of [12, Theorem 15]. There is a little discrepancy between our theorem and the latter theorem; in fact, the "only if" part of the latter is contained in that part of ours (and its left analogy), but the similar is not the case for the "if" parts.

[16] Generally, in a ring satisfying both the left and the right minimum conditions, a two-sided ideal which is both left and right principal is generated by a common element. See Nakayama [13, Lemma 1].

$A/\mathfrak{z}$-$A/\mathfrak{z}^*$-module. Hence, in order that $A/\mathfrak{z}$ be Frobenius it is necessary and sufficient, by virtue of Theorems 14 and 15, that $A/\mathfrak{z}$ be, as left ($A/\mathfrak{z}$- or) A-module, isomorphic to $r(\mathfrak{z})$, or what is the same thing, that there exist an element c in $r(\mathfrak{z})$ such that $Ac = r(\mathfrak{z})$ and $l(c) = \mathfrak{z}$; but the latter equality means $cA = r(\mathfrak{z})$, because $r(l(c)) = r(l(cA)) = cA$ and $l(r(\mathfrak{z})) = \mathfrak{z}$. The last assertion is now an immediate consequence of the fact that $A/\mathfrak{z}$ and $A/\mathfrak{z}^*$ are, in this case, the endomorphism rings of the left A-modules $A/\mathfrak{z}$ and $r(\mathfrak{z})$ respectively; in fact, we have an isomorphism between these two rings by associating $a \in A$ with such $a^* \in A^*$ that $ac = ca^*$.

Finally, we would like to refer to the existence of finitely generated injective modules. Let r be the index of nilpotency of N. Consider a factor module $N^i - N^{i+1}$, $1 \leqq i < r$, and any left A-module M. Then the module $\mathrm{Hom}_A(N^i - N^{i+1}, M)$ consisting of all A-homomorphisms h of $N^i - N^{i+1}$ into M can be converted into a left A-module by setting ah, $a \in A$, to be the mapping $x \to (xa)h$, $x \in N^i - N^{i+1}$ (cf. [1, II. 3.]). Now, Rosenberg and Zelinsky proved the following theorem ([14, Theorem 1]): *The minimal injective extension $\hat{M}$ of M is finitely generated if and only if so is every left A-module* $\mathrm{Hom}_A(N^i - N^{i+1}, M)$, $i = 1, 2, \cdots, r-1$. Moreover, they gave, by making use of this theorem, an example for a ring A (satisfying the left minimum condition but) having no finitely generated injective left-module ($\neq 0$). We shall, however, need later only the following special case of the above theorem:

PROPOSITION 9. *Let A be a commutative ring satisfying the minimum condition for ideals, and let M be a finitely generated A-module. Then the minimal injective extension of M is also finitely generated.*

For, $\mathrm{Hom}_A(N^i - N^{i+1}, M)$ may be, in this case, interpreted as the dual module of $N^i - N^{i+1}$ with respect to M (when M is regarded as a two-sided A-module in the natural manner), and therefore is finitely generated, as can easily be seen from the finite generatedness for both modules $N^i - N^{i+1}$ and M.

Addendum. It is perhaps of some interest, in connection with Theorem 7, to add the following theorem, which holds for an arbitrary ring A:

THEOREM 17. *Let M be a left A-module and $Q = \hat{M}$ its minimal injective extension. Let $\mathfrak{z}$ be a two-sided ideal of A. Then $r_Q(\mathfrak{z})$, when regarded as a left-module of $A/\mathfrak{z}$, is the minimal injective extension of the left $A/\mathfrak{z}$-module $r_M(\mathfrak{z})$.*

Proof. It is easy to see that $r_Q(\mathfrak{z})$ is $A/\mathfrak{z}$-injective. So it suffices to show that $r_Q(\mathfrak{z})$ is, as $A/\mathfrak{z}$-module, an essential extension of $r_M(\mathfrak{z})$. However,

this follows immediately from the fact that $M' \cap M = M' \cap r_Q(\mathfrak{z}) \cap M = M' \cap r_M(\mathfrak{z})$ for every A-submodule M' of $r_Q(\mathfrak{z})$.

COROLLARY. *Let $\mathfrak{z}$ be a two-sided ideal of A, and let M be an injective left $A/\mathfrak{z}$-module. Looking upon M as an A-module, let Q be the minimal A-injective extension of M. Then we have $r_Q(\mathfrak{z}) = M$.*

5. The canonical module for an algebra. Changing letters, let Φ be a commutative ring satisfying the minimum condition (for ideals) and let $\mathfrak{n}$ be the radical of Φ. Denote by F the minimal injective extension of the (completely reducible) factor module $\Phi - \mathfrak{n}$, and let us call it the *canonical Φ-module.*

PROPOSITION 10. *The canonical Φ-module F is finitely generated, and Φ coincides with the Φ-endomorphism ring of F; in other words, F is a Frobenius Φ-module, when regarded as a two-sided Φ-module in the natural manner.*

Proof. The finite generatedness of F follows from Proposition 9. Let Φ^* be the Φ-endomorphism ring of F. Then, by Theorem 14, Φ^* satisfies the right minimum condition and F is a Frobenius two-sided Φ-Φ^*-module. Furthermore, since $r_F(\mathfrak{n}) = (l_F(\mathfrak{n}) =) l_F(\mathfrak{n}\Phi^*)$, it follows from Theorem 7 that $r_F(\mathfrak{n})$ is Frobenius as two-sided $\Phi/\mathfrak{n}$-$\Phi^*/\mathfrak{n}\Phi^*$-modlue. On the other hand, the Φ-socle $r_F(\mathfrak{n})$ of F is (isomorphic to) $\Phi - \mathfrak{n}$, so that $\Phi/\mathfrak{n}$ coincides with the Φ-endomorphism ring of $r_F(\mathfrak{n})$. This implies that $\Phi^*/\mathfrak{n}\Phi^* = \Phi/\mathfrak{n}$, i.e., $\Phi^* = \Phi + \mathfrak{n}\Phi^*$; but since $\mathfrak{n}$ is nilpotent, we can immediately deduce that $\Phi^* = \Phi$.

Combining Proposition 10 again with Theorem 7, we have

COROLLARY. *Ideals $\mathfrak{a}$ of Φ and Φ-submodules F_0 of the canonical Φ-module F correspond one-to-one by the annihilator relations, and in this case, F_0 is regarded as the canonical $\Phi/\mathfrak{a}$-module in the natural way.*

Let now M be a finitely generated Φ-module. According to Theorem 8, the dual module $\tilde{M} = \mathrm{Hom}_\Phi(M, F)$ of M with respect to F is also a finitely generated Φ-module, and M coincides with the dual module of $\tilde{M}$; furthermore, Φ-submodules L of M and R of $\tilde{M}$ correspond one-to-one by the annihilator relations, so that L and $\tilde{M} - R$ are dual modules of each other.

We shall, from now on, assume that A is an *algebra* over Φ in the sense that A is a ring and at the same time a finitely generated Φ-module such that $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for $\alpha \in \Phi$, a, $b \in A$.[17] Then A satisfies evi-

[17] It should be noted that here the notion of algebras is free of such a condition as that they have linearly independent bases, or more generally that they are projective,

dently the left as well as the right minimum condition. So we may use notations N, $\bar{A}=A/N(=A-N)$, k, $f(\kappa)$, e_κ, etc. in the same meanings as in the preceding section. Let now M be a finitely generated left (or right) A-module. Looking upon M as a finitely generated Φ-module in the natural way, we consider its dual module $\tilde{M}$ (with respect to F). We may however convert $\tilde{M}$ into a right (or left) A-module by setting χa (or $a\chi$), $\chi \in \tilde{M}$, $a \in A$, to be the mapping $x \to \chi(ax)$ (or $x \to \chi(xa)$), $x \in M$. The A-module $\tilde{M}$ is obviously finitely generated, and will be called the *Φ-dual module* of (the A-module) M. It is then easy to see that M may be regarded as the Φ-dual module of $\tilde{M}$ in the natural manner and there exists a one-to-one correspondence between A-submodules L of M and R of $\tilde{M}$ by the annihilator relations, so that L and $\tilde{M}-R$, $M-L$ and R are Φ-dual modules of each other[18]; the corresponding L and R we shall call the *Φ-annihilators* of R and L respectively. From this it follows in particular that $\tilde{M}$ is irreducible if and only if so is M, and indeed we have

LEMMA 2. *The Φ-dual module of $\bar{A}\bar{e}_\kappa$ is isomorphic to $\bar{e}_\kappa\bar{A}$, for each κ.*

For, if χ is an element of the Φ-dual module $\tilde{M}$ of $M=\bar{A}\bar{e}_\kappa$ and if $\lambda \neq \kappa$, then χe_λ maps M onto $\chi(e_\lambda M)=\chi(\bar{e}_\lambda \bar{A}\bar{e}_\kappa)=0$, that is, $\tilde{M}e_\lambda=0$.

Let Q be a two-sided A-module (which is element-wise commutative with Φ). Then it is clear that the Φ-dual module $\tilde{Q}$ of Q is (not only a right and a left but also) a two-sided A-module too. We now call Q a *canonical two-sided A-module* if $\tilde{Q}$ is isomorphic to (the two-sided A-module) A itself, or equivalently, if Q is isomorphic to the Φ-dual module $\tilde{A}$ of A.

THEOREM 18. *In order that a two-sided A-module Q be canonical it is necessary and sufficient that Q be faithful and have a Φ-homomorphism μ into F such that $\mu(au)=\mu(ua)$ for $a \in A$ and $u \in Q$ and that $\mu(L)\neq 0$ for every non-zero left A-submodule L of Q.*

Proof. That $\tilde{Q}\cong A$ means the existence of an element μ of $\tilde{Q}$ satisfying the following three conditions: (1) $a\mu=\mu a$, $a \in A$, (2) $\mu A=\tilde{Q}$, (3) $\mu a=0$, $a \in A$, implies $a=0$. However, the second condition (2) is equivalent to saying that the Φ-annihilator of μA is 0, that is, $\mu(Au)=0$, $u \in Q$, implies $u=0$, while the third condition (3) means nothing but that $\mu(aQ)=0$, $a \in A$,

with respect to their base rings, which was asumed throughout in both the papers [3] and Kasch [8] (although we impose stronger restrictions on base rings in our case).

[18] In the special case where Φ is a field, F coincides necessarily with Φ itself, and therefore the concept of Φ-dual modules accords with that of dual representation spaces; indeed, the above relationship between Φ-dual modules turns, in this case, to the known relationship mentioned at the beginning of our introduction.

implies $a=0$, which, under both the assumptions (1) and (2), is evidently equivalent to the faithfulness of Q.

LEMMA 3. *For any left (or right) ideal of A, its right (or left) annihilator in $\tilde{A}$ coincides with its Φ-annihilator.*

Proof. Suppose that χ is an element of the right annihilator in $\tilde{A}$ of the given left ideal $\mathfrak{l}$. Then $\chi(a)=(a\chi)(1)=0$ for all $a\in\mathfrak{l}$. Assume conversely that χ is in the Φ-annihilator of $\mathfrak{l}$. Then, for any $a\in\mathfrak{l}$ and $x\in A$, $(a\chi)(x)=\chi(xa)=0$; i.e., $a\chi=0$.

THEOREM 19. *Let Q be the canonical two-sided A-module. Then Q is Frobenius. Moreover, for any two-sided ideal $\mathfrak{z}$ of A, its right and left annihilators in Q coincide, and the common annihilator, when regarded as a two-sided $A/\mathfrak{z}$-module, is canonical.*

Proof. We may of course assume that $Q=\tilde{A}$. Let $\mathfrak{l}$ be a maximal left ideal of A and suppose that $A-\mathfrak{l}\cong\bar{A}\bar{e}_{\kappa}$. Then the right annihilator $r_Q(\mathfrak{l})$ is, as right A-module, isomorphic to the right-dual module of $\bar{A}\bar{e}_{\kappa}$. On the other hand, $r_Q(\mathfrak{l})$ may, since it coincides with the Φ-annihilator of $\mathfrak{l}$ by Lemma 3, be regarded as the Φ-dual module of $A-\mathfrak{l}$, so that we have $r_Q(\mathfrak{l})\cong\bar{e}_{\kappa}\bar{A}$ by Lemma 2. The similar holds, by symmetry, for every maximal right ideal of A. In view of the fact that the capacities of both irreducible modules $\bar{A}\bar{e}_{\kappa}$ and $\bar{e}_{\kappa}\bar{A}$ coincide with $f(\kappa)$, these, together with the faithfulness of Q (Theorem 18), show that Q is a Frobenius two-sided A-module. Now, Lemma 3 again assures that both the right and the left annihilators $r_Q(\mathfrak{z})$ and $l_Q(\mathfrak{z})$ of a two-sided ideal $\mathfrak{z}$ coincide with the Φ-annihilator of $\mathfrak{z}$ and moreover $\mathfrak{z}$ is the left as well as the right annihilator (in A) of the common annihilator $r_Q(\mathfrak{z})=l_Q(\mathfrak{z})$. The remaining part of our assertion follows now from Theorem 18, because if μ is a Φ-homomorphism of Q into F as in the theorem then the restriction of μ in the common annihilator satifies the similar conditions as μ does.

We now prove the following fundamental

THEOREM 20. *Let Q be a canonical two-sided A-module. Then, for any finitely generated left A-module M, the right-dual module $M^*=\mathrm{Hom}_A(M,Q)$ of M with respect to Q is, as right A-module, isomorphic to the Φ-dual module $\tilde{M}$ of M, by associating each $f\in M^*$ with the composite mapping of f, μ, where μ is a Φ-homomorphism of Q into F as in Theorem 18.*

Proof. For any $f\in M^*$, we denote by $\tilde{f}$ the composite mapping of f, μ: $\tilde{f}(x)=\mu(xf)$, $x\in M$. Then $\tilde{f}\in\tilde{M}$, and $(\tilde{f}a)(x)=\tilde{f}(ax)=\mu(axf)=\mu(xfa)$,

i.e., $\bar{f}a = \widetilde{fa}$ for all $a \in A$, which shows that the mapping $f \to \bar{f}$ gives an A-homomorphism of M^* into $\bar{M}$. Suppose now $\bar{f} = 0$, that is, $\mu(Mf) = 0$. Since Mf is a left A-submodule of Q, it follows that $Mf = 0$, whence $f = 0$. This means that the mapping $f \to \bar{f}$ is one-to-one. Suppose, on the other hand, that $\mu(xM^*) = 0$. Since xM^* is a right A-submodule of Q, it follows also that $xM^* = 0$ (because if $u \in xM^*$ then $\mu(Au) = \mu(uA) = 0$); but since Q is (quasi-)Frobenius by Theorem 19, it follows that $x = 0$ (Theorem 8). This means that the Φ-annihilator of the homomorphic image of M^* (under the mapping $f \to \bar{f}$) is 0, that is, the image fills up $\bar{M}$. Thus the proof is completed.

Now, let Γ denote the center of A. Then Γ is a commutative algebra over Φ, and in particular it satisfies the minimum condition (for ideals). Let C be the canonical Γ-module, that is, the minimal (Γ-)injective extension of the factor module of Γ modulo its radical. Consider, on the other hand, the Φ-dual module $\bar{\Gamma}$ of (the Γ-module) Γ. Then $\bar{\Gamma}$ (is element-wise commutative with Γ and) is, by Theorem 19, a Frobenius Γ-module, Hence, it follows from Theorem 14 that $\bar{\Gamma}$ is isomorphic to C, or what is the same thing, C is a canonical two-sided module of (the algebra) Γ. Then C has, according to Theorem 18, a Φ-homomorphism ν into F such that $\nu(S) \neq 0$ for every non-zero Γ-submodule S of C. Now, looking upon A as an algebra over Γ in the natural way, we consider a canonical two-sided A-module Q. Then Q has, by Theorem 18, a Γ-homomorphism μ into C such that $\mu(au) = \mu(ua)$, $a \in A$, $u \in Q$, and $\mu(L) \neq 0$ for every non-zero left A-submodule L of Q. It is then easy to see that the composite mapping $u \to \nu(\mu(u))$, $u \in Q$, is a Φ-homomorphism of Q into F and fulfills the same conditions as μ, so that Q is, again by Theorem 18, a canonical two-sided module of the algebra A over Φ. We have thus proved the following

THEOREM 21. *The canonical two-sided A-module is uniquely determined, up to isomorphisms, by the ring A, and is independent of the choice of the base ring.*

Let us now call A a *symmetric algebra* if it is canonical when regarded as a two-sided A-module. The following theorem, which follows immediately from Theorem 18, shows that the notion accords with the old one in the case of algebras over a field (cf. Nakayama [11]):

THEOREM 22. *An algebra A over Φ is symmetric if and only if A has a Φ-homomorphism μ into F such that $\mu(ab) = \mu(ba)$ for $a, b \in A$ and $\mu(\mathfrak{l}) \neq 0$ for any non-zero left ideal $\mathfrak{l}$ of A.*

Finally, we shall give characterizations of Frobenius modules and Fro-

benius algebras in terms of the canonical module. For this purpose, we consider a two-sided A-module Q and an automorphism ϕ of A. For any $u \in Q$ and $a \in A$, we define a new product by setting $u*a = ua^{\phi^{-1}}$. Then it is easy to see that Q is converted into a new two-sided A-module under this multiplication, if the left multiplication of elements of A on Q is taken to be the original one. We shall denote this module by (Q, ϕ).

THEOREM 23. *Let Q be the canonical two-sided A-module. Then a two-sided A-module is Frobenius if and only if it is isomorphic to (Q, ϕ) with some automorphism ϕ of A; and, in this case, ϕ is unique up to inner automorphisms.*

Proof. Let Q' be a Frobenius two-sided A-module. In view of the fact that Q is also Frobenius (Theorem 19), Theorem 14 implies that Q' is, as left A-module, isomorphic to Q and moreover A, as right operator-ring, coincides with the endomorphism ring of Q' as well as of Q. Therefore, if $u \rightarrow u'$, $u \in Q$, is an isomorphism of Q onto Q', we can find an automorphism ϕ of A so that $(ua)' = u'a^{\phi}$, or equivalently, $(u*a)'(= (ua^{\phi^{-1}})') = u'a$ for $u \in Q$, $a \in A$, showing that Q' is isomorphic to (Q, ϕ). That conversely every (Q, ϕ) is Frobenius may also be seen quite easily from Theorem 14, while that two modules (Q, ϕ) and (Q, ψ), with automorphisms ϕ, ψ, are isomorphic if and only if $\phi\psi^{-1}$ is an inner automorphism follows immediately from the fact that any isomorphism betwen the above modules can be given by the right multpilication (in the original sense) of a regular element of A.

THEOREM 24. *An algebra A over Φ is Frobenius if and only if A has a Φ-homomorphism μ into F such that $\mu(\mathrm{I}) \neq 0$ for any non-zero left ideal I. And, in this case, there exists an automorphism ϕ of A such that $\mu(ab) = \mu(ba^{\phi})$ for a, $b \in A$.* (Cf. [11] and [12, Theorem 1].)

Proof. Since the Φ-dual module $\tilde{A}$ of A is Frobenius (Theorem 19), it is evident from Theorems 14 and 15 that A is Frobenius if and only if A is isomorphic with $\tilde{A}$ as left A-modules. But if we observe the fact that A and $\tilde{A}$ have the same composition length with respect to Φ (by the Corollary of Proposition 2), it is easy to see that the latter condition may be replaced by the weaker condition that $\tilde{A}$ contains an isomorphic image of A, i.e., there exists a $\mu \in \tilde{A}$ such that $a\mu = 0$, $a \in A$, implies $a = 0$, and this proves the first part of our theorem (because $a\mu = 0$ means nothing but $\mu(Aa) = 0$). Now, since $A\mu = \tilde{A}$ and $\tilde{A}$ is faithful, it follows again from the equality of Φ-lengths of A and $\tilde{A}$ that $\mu A = \tilde{A}$ too. Thus, by associating each $a \in A$ with an $a^* \in A$ such that $a^*\mu = \mu a$, we obtain the desired automorphism $\phi: a \rightarrow a^*$.

YALE UNIVERSITY AND HOKKAIDO UNIVERSITY.

REFERENCES.

[1] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University, 1956.

[2] B. Eckmann and A. Schopf, "Über injektive Moduln," *Archiv der Mathematik*, vol. 4 (1953), pp. 75-78.

[3] S. Eilenberg and T. Nakayama, "On the dimension of modules and algebras," II, *Nagoya Mathematical Journal*, vol. 9 (1955), pp. 1-16.

[4] M. Hall, "A type of algebraic closure," *Annals of Mathematics*, vol. 40 (1939), pp. 360-369.

[5] M. Ikeda, "A characterization of quasi-Frobenius rings," *Osaka Mathematical Journal*, vol. 4 (1952), pp. 203-210.

[6] ——— and T. Nakayama, "On some characteristic properties of quasi-Frobenius and regular rings," *Proceedings of the American Mathematical Society*, vol. 5 (1954), pp. 15-19.

[7] N. Jacobson, *Structure of Rings*, American Mathematical Society Colloquium Publications, 1956.

[8] F. Kasch, "Grundlagen einer Theorie der Frobeniuserweiterungen," *Mathematische Annalen*, vol. 127 (1954), pp. 453-474.

[9] K. Morita and H. Tachikawa, "Character modules, submodules of a free module, and quasi-Frobenius rings," *Mathematische Zeitschrift*, vol. 65 (1956), pp. 414-428.

[10] H. Nagao and T. Nakayama, "On the structure of (M_0)- and (M_u)-modules," *Mathematische Zeitschrift*, vol. 59 (1953), pp. 164-170.

[11] T. Nakayama, "On Frobeniusean algebras, I," *Annals of Mathematics*, vol. 40 (1939), pp. 611-633.

[12] ———, "On Frobeniusean algebras, II," *Annals of Mathematics*, vol. 42 (1941), pp. 1-21.

[13] ———, "Note on uni-serial and generalized uni-serial rings," *Proceedings of the Imperial Academy of Tokyo*, vol. 16 (1940), pp. 285-289.

[14] A. Rosenberg and D. Zelinsky, "Finiteness of the injective hull," forthcoming in *Mathematische Zeitschrift*.

After the submission of this manuscript, the writer has learned of the publication of the following three papers, in which many similarities are found with the present work:

[a] K. Morita, Y. Kawada and H. Tachikawa, "On injective modules," *Mathematische Zeitschrift*, vol. 68 (1957), pp. 217-226.

[b] H. Tachikawa, "Duality theorem of character modules for rings with minimum condition," *Mathematische Zeitschrift*, vol. 68 (1958), pp. 479-487.

[c] K. Morita, "Duality for modules and its applications to the theory of rings with minimum condition," *Science Reports of the Tokyo Kyoiku Daigaku*, vol. 6 (1958), pp. 83-142.

Indeed, most of our principal results are also obtained in these papers; cf. in particular, [c, Theorem 1. 1] and [c, Theorem 6. 3].

ERRATA.

à l'article: *Sur les revêtements non ramifiés des variétés algébriques* (vol. 79, 1957, pp. 319-330).

par Serge Lang et Jean-Pierre Serre.

Soit $f\colon U \to V$ un revêtement d'une variété algébrique V, soit V' une sous-variété irréductible de V, et soient U_i' les composantes de $f^{-1}(V')$. D'après un théorème de Krull, les facteurs séparables $[U_i'\colon V']_s$ des degrés $[U_i'\colon V']$ vérifient l'inégalité:

(1) $$\Sigma[U_i'\colon V']_s \leqq [U\colon V].$$

Si de plus (1) est une égalité, on a $[U_i'\colon V']_s = [U_i'\colon V']$.

Dans l'article précité, nous avons écrit à la place de (1) la formule incorrecte suivante:

(2) $$\Sigma[U_i'\colon V'] \leqq [U\colon V].$$

Cette erreur nous a été signalée par M. Greenberg. Elle n'est d'ailleurs d'aucune conséquence pour la suite de l'article: l'inégalité (2) n'intervenait que dans le lemme 1, et peut y être remplacée par (1), à condition de définir les entiers n_i par $n_i = [U_i'\colon V']_s$.

Quant à la formule (2), elle est vraie si V' est *simple* sur V, en vertu de la théorie des intersections (voir Samuel, *Algèbre locale*, p. 32, cor. 2). Elle est par contre inexacte dans le cas général, comme le montre l'exemple suivant:

Soit X une variété normale, définie sur un corps de caractéristique $p > 0$. Soit $U = X^p$ (produit de la variété p fois avec elle-même), et soit $V = X^{(p)}$ (puissance symétrique p-uple de X); la variété V est quotient de U par le groupe symétrique de degré p, ce qui montre que $[U\colon V] = p!$. Prenons pour V' l'image de la diagonale Δ de X^p; l'image réciproque de V' dans U est Δ, et l'application $\Delta \to V'$ est bijective; toutefois, *ce n'est pas un isomorphisme*; on constate en effet, par application du théorème des fonctions symétriques, que les fonction rationnelles sur V' s'identifient aux puissances p-ièmes des fonctions rationnelles sur Δ. On a donc $[\Delta\colon V'] = p^{\dim. X}$, et l'inégalité (2) est en défaut si l'on s'arrange pour que $p^{\dim. X} > p!$; l'exemple le plus simple est $p = \dim. X = 2$. On notera que l'on peut même choisir U

non singulière (par contre, on sait que. $V = X^{(p)}$ est toujours singulière lorsque dim. $X \geqq 2$).

Traduit en termes d'algèbre locale, l'exemple précédent fournit deux anneaux locaux normaux A et B, avec B entier et galoisien sur A, tels que, si k_A et k_B désignent leurs corps des restes, on ait:

$$[k_B : k_A] > [B : A].$$

En prenant une infinité de variables on peut même s'arranger pour que $[k_B : k_A] = \infty$, mais les anneaux A et B ne sont alors plus noethériens.

Correction to the paper "On some invariants of cyclotomic fields" by K. IWASAWA, this Journal, vol. 80 (1958), pp. 773-783.

Lemma 2 on p. 779 should be replaced by the following:

LEMMA 2. *Suppose that*

$$\sum a_\xi \zeta_{n+1}{}^{\xi} \equiv 0 \bmod. p^s \qquad (\xi \text{ in } U \bmod. U_n)$$

with a_ξ *in* Q_p. *Then* $a_\xi \equiv a_\omega \bmod. p^s$ *whenever* $\xi \equiv \omega \bmod. U_{n-1}$.

Using this lemma, it follows from (8), after a simple computation, that $S_n(\chi) \equiv 0 \bmod. p$ for any character χ of U satisfying $\chi(U_n) = 1$, $\chi(U_{n-1}) \neq 1$, $\chi(\eta) = \eta^{-a}$. Hence (8) implies $\mu > 0$.

SECONDARY COHOMOLOGY OPERATIONS: TWO FORMULAS.* [1]

By F. P. PETERSON and N. STEIN.

Introduction. In the past decade, there have been many important applications of algebraic topology involving such primary cohomology operations as cup products and the Steenrod reduced powers. Recently, it has become clear that many more problems can be attacked by considering secondary and higher order cohomology operations. Unfortunately, these are more difficult to compute than primary operations. In this paper, we give two formulas relating secondary cohomology operations to primary and functional primary cohomology operations, thus reducing the problem of computation to somewhat simpler problems.

In Chapter one, we discuss higher order cohomology operations, paying particular attention to the difficulties which arise in the non-stable cases. For example, in such cases the values of a secondary cohomology operation may be cosets of subgroups which depend on the variable to which the operation is applied and not only on the operation itself. In some cases they may be subsets of a group which are not necessarily cosets.

In Chapter two, we prove the following two formulas (stated here in the stable form). Let Φ be a secondary operation coming from the relation $\theta'\theta = 0$, where $\theta \in H^{n'+1}(\pi, n; \pi')$ and $\theta' \in H^{q+1}(\pi', n'+1; G)$. 1) Let $f: L \to K$ and let $u \in H^n(K; \pi)$ be such that $f^*(u) = 0$ and $\theta(u) = 0$. Then $f^*\Phi(u) = {}^1\theta'(\theta_f(u)) \in H^q(L; G)/{}^1\theta' f^*(H^{n'}(K; \pi'))$, where ${}^1\theta'$ denotes the suspension of θ'. 2) Let $f: L \to K$ and let $u \in H^n(K; \pi)$ be such that $f^*\theta(u) = 0$. Then $\Phi(f^*(u)) = \theta'_f(\theta(u)) \in H^q(L; G)/{}^1\theta'(H^{n'}(L; \pi')) + f^*(H^q(K; G))$. We also prove analogs of these formulas for some non-stable operations and for operations on more than one variable. There are similar formulas for higher order cohomology operations, but we shall not discuss them here.

In Chapter three, we give examples of applications of these two formulas to finding relations on secondary cohomology operations; e.g. we show that

* Transferred from *Annals of Mathematics*, September 27, 1958.

[1] This research was supported in part by the United States Air Force under Contract No. AF 18(600)-1383, and Contract No. AF 18(600)-1494, monitored by AF Office of Scientific Research, Air Research and Development Command.

$\mathrm{Sq}^2\Psi_n = 0$ for n odd, where Ψ_n is the secondary operation needed to classify maps into complex projective spaces (see Stein's thesis [13]). Finally, we show how the knowledge of secondary cohomology operations in the base of a fibre space gives information on primary cohomology operatins in the total space.

Throughout this paper, all statements refer to the total singular complexes of the spaces involved, and all homotopies are singular homotopies [16]. For simplicity, we will always use the geometric language.

A preliminary account of these results was given in [8].

Chapter I. Cohomology Operations.

1. Fibre spaces and principal fibre spaces. We will assume throughout this paper that the spaces are simply connected.

For any two spaces X and Y with base points $x \in X$, $y \in Y$, we denote by $\pi(X;Y)$ the set of homotopy classes of maps $(X,x) \to (Y,y)$. In many cases, e.g. whenever Y is a space of loops, $\pi(X;Y)$ has a natural group structure. In any case it contains a neutral element—the homotopy class of the constant map. We denote by ${}^1X$ the space of loops in X based at x and define ${}^rX = {}^1({}^{r-1}X)$. Finally, we denote by SX the reduced suspension of X and define $S^rX = S(S^{r-1}X)$.

Let $p\colon E \to B$ be a fibre space in the sense of Serre; let $b \in B$ and $e \in F = p^{-1}(b)$ be base points and let $i\colon F \to E$ be the inclusion map. Then according to Lemma 2.1 of [7], we have, for any space X, an exact sequence

$$(1.1) \qquad \cdots \to \pi(X;{}^rF) \xrightarrow{({}^ri)_\#} \pi(X;{}^rE) \xrightarrow{({}^rp)_\#} \pi(X;{}^rB) \to \pi(X;{}^{r-1}F) \to$$
$$\cdots \to \pi(X;F) \xrightarrow{i_\#} \pi(X;E) \xrightarrow{p_\#} \pi(X;B).$$

We now recall the notion of principal fibre space [9].

Definition. Let $p\colon E \to B$, b, e, and F be as above. We assume that F is a monoid (i.e. a topological semi-group with identity), and that there is given a map

$$\mu\colon F \times E \to E$$

such that the following diagrams are commutative (m is the multiplication in F and π is the projection onto the second factor):

$$\begin{array}{ccc} F\times F & \xrightarrow{m} & F \\ {\scriptstyle 1\times i}\downarrow & & \downarrow{\scriptstyle i} \\ F\times E & \xrightarrow{\mu} & E \end{array}$$

$$\begin{array}{ccc} F\times E & \xrightarrow{\mu} & E \\ {\scriptstyle 1\times p}\downarrow & & \downarrow{\scriptstyle p} \\ F\times B & \xrightarrow{\pi} & B. \end{array}$$

Let $E^* = \{(e_1, e_2) \in E \times E \mid p(e_1) = p(e_2)\}$ and defines maps

$$p_i\colon E^* \to E, \qquad i = 1, 2,$$

by setting $p_i(e_1, e_2) = e_i$. We assume that there is given a map

$$h : E^* \to F$$

such that the following diagram is commutative up to homotopy:

$$\begin{tikzcd} E^* \arrow[r, "{(h, p_1)}"] \arrow[dr, "p_2"'] & F \times E \arrow[d, "\mu"] \\ & E \end{tikzcd}$$

In this case, we say that we have a *principal fibre space.*

As was remarked in [9], the Moore path space is a principal fibre space and any fibre space which is induced from a principal fibre space by a map, is itself a principal fibre space.

It is easy to see that if F admits a classifying space $\chi(F)$, i.e. if there is a principal fiber space with fibre F, base space $\chi(F)$, and acyclic total space, from which any principal fibre space with fibre F is induced by a continuous map χ of its base into $\chi(F)$, then the exact sequence (1.1) can be extended by one term so as to end with $\xrightarrow{p_\#} \pi(X; B) \xrightarrow{\chi_\#} \pi(X; \chi(F))$. In particular, this holds whenever F is a loop-space.

We recall for later use Lemma 4.1 of [9].

LEMMA 1.2. *Let (E, p, B, F, μ, h) be a principal fibre space and let X be any space. Let $v, v' \in \pi(X; E)$. Then $p_\#(v) = p_\#(v')$ if and only if there exists $w \in \pi(X; F)$ such that $\mu_\#(w, v) = v'$.* [Here we use

$$\pi(X;F) \times \pi(X;E) = \pi(X;F \times E) \xrightarrow{\mu_\#} \pi(X;E).]$$

Also for later use we point out an obvious lemma.

LEMMA 1.3. *Under the same hypotheses, we have a commutative diagram*

$$\begin{tikzcd}
\pi(X;F \times E) \times H^i(E;G) \arrow[r, "\mu_\# \times 1"] \arrow[d, "1 \times \mu^*"'] & \pi(X;E) \times H^i(E;G) \arrow[d] \\
\pi(X;F \times E) \times H^i(F \times E;G) \arrow[r] & H^i(X;G)
\end{tikzcd}$$

where the unlabelled arrows indicate operation of the first factor in the direct product on the second.

We note that it can be seen easily that the Moore path space is a homotopy associative principal fibre space in the sense that the following diagram is commutative up to homotopy:

$$\begin{tikzcd}
F \times F \times E \arrow[r, "1 \times \mu"] \arrow[d, "m \times 1"'] & F \times E \arrow[d, "\mu"] \\
F \times E \arrow[r, "\mu"] & E.
\end{tikzcd}$$

Furthermore, a principal fibre space induced from a homotopy associative one is clearly homotopy associative. Finally, in a homotopy associative principal fibre space the following diagram is easily seen to be commutative up to homotopy (f is the identity of F, π denotes projection onto the second factor, and j is the inclusion):

$$\begin{tikzcd}
f \times E \arrow[r, "j \times 1"] \arrow[dr, "\pi"'] & F \times E \arrow[d, "\mu"] \\
 & E.
\end{tikzcd}$$

2. Postnikov spaces and their fibrations. The Postnikov scheme for determining the homotopy type of complexes [10] is based on the study of spaces with a finite number of non-trivial homotopy groups. The homotopy type of such a space is not uniquely determined by these groups but depends also on certain auxiliary invariants, known as k-invariants or Postnikov invariants. We will describe an inductive procedure for constructing the

Postnikov spaces which exhibits them as homotopy associative principal fibre spaces and in which the dependence on the k-invariants is indicated.

We recall first that for the case of a space with only one non-trivial homotopy group, i. e. an Eilenberg-MacLane space, the homotopy type is determined by the group. We assume that we are given a Postnikov space $\mathfrak{P}$ and we wish to construct a new space $\mathfrak{P}'$ which has the same homotopy groups as $\mathfrak{P}$ except in one dimension n which is assumed to be larger than the dimension of any non-trivial homotopy group of $\mathfrak{P}$, and that $\pi_n(\mathfrak{P}') \approx \pi$. For this, we consider the space $K(\pi, n+1)$ and the space E of Moore paths in $K(\pi, n+1)$ with fixed initial point, which according to § 1 is a principal fibre space over $K(\pi, n+1)$ with fibre the space of loops in $K(\pi, n+1)$, i. e. $K(\pi, n)$. For each map of $\mathfrak{P}$ into $K(\pi, n+1)$ we get an induced principal fibre space $\mathfrak{P}'$ with base $\mathfrak{P}$ and fibre $K(\pi, n)$.

$$\begin{tikzcd} K(\pi, n) \arrow[r] & \mathfrak{P}' \arrow[r] \arrow[d] & E \arrow[d] & K(\pi, n) \arrow[l] \\ & \mathfrak{P} \arrow[r] & K(\pi, n+1). & \end{tikzcd}$$

The homotopy sequence of this fibre space shows that $\mathfrak{P}'$ has the right homotopy groups. Altering the map $\mathfrak{P} \to K(\pi, n+1)$ within its homotopy class does not change the homotopy type of $\mathfrak{P}'$. According to the Hopf-Whitney theorem, the homotopy classes of maps $\mathfrak{P} \to K(\pi, n+1)$ are in natural one-one correspondence with the elements of the group $H^{n+1}(\mathfrak{P}; \pi)$. The element of this group corersponding to the map $\mathfrak{P} \to K(\pi, n+1)$ is the new k-invariant.

We remark that it is clear from this construction that the homotopy type of $\mathfrak{P}'$ is determined by the Postnikov system, i. e. the sequence of homotopy groups and k-invariants. However, it is unfortunately over-determined by this information in the sense that different Postnikov systems may correspond to the same homotopy type. Of course the homotopy groups cannot be altered beyond isomorphism but it is still an open question to say how much the k-invariants can be changed without affecting the homotopy type.

We will use the notation $\mathfrak{P}(\pi, n; \pi', n', \theta; \cdots; \pi^{(q)}, n^{(q)}, \theta^{(q-1)})$ for a space with homotopy groups $\pi^{(i)}$ in dimension $n^{(i)}$ and k-invariants

$$\theta^{(i-1)} \in H^{n^{(i)}+1}(\mathfrak{P}(\pi, n; \cdots; \pi^{(i-1)}, n^{(i-1)}, \theta^{(i-2)}); \pi^{(i)}).$$

3. Cohomology operations. Serre has remarked in [11] that due to the Hopf-Whitney theorem we can identify a universally defined cohomology operation with an element of a cohomology group of an Eilenberg-MacLane space. Motivated by this result, we give here a treatment of general cohomology operations. Our treatment gives a procedure for constructing these operations but we feel that it would be of interest to give an axiomatic characterization of them. J. F. Adams has recently given such a characterization for stable secondary operations.

We describe briefly the treatment of primary cohomology operations. Such an operation is uniquely determined by a cohomology class in an Eilenberg-MacLane space as follows: Let $\phi \in H^q(\pi, n; G)$. Let X be a space and let $h \in H^n(X; \pi)$. The homotopy classes of maps of X into $K(\pi, n)$ are in one-one correspondence with the elements of $H^n(X; \pi)$, and the correspondence is given by $f \leftrightarrow f^*(\iota)$, where $\iota \in H^n(\pi, n; \pi)$ is the basic class. Let $f\colon X \to K(\pi, n)$ be a map which corresponds to h, i. e. such that $f^*(\iota) = h$. Then we define $\phi(h) = f^*(\phi)$. Thus for any space X, ϕ is a natural function from $H^n(X; \pi)$ to $H^q(X; G)$.

For clarity, we will now describe the case of secondary operations and then show how to treat the general case. Let $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$ be a Postnikov space, and let $\phi \in H^q(\mathfrak{P}; G)$. According to § 2, $\mathfrak{P}$ is a principal fibre space over $K(\pi, n)$ with fibre $K(\pi', n')$ and $K(\pi', n'+1)$ is a classifying space for this fibre space. For any space X, we have the exact sequence (1.1) with the extra term described at the end of § 1. We rewrite this sequence identifying $\pi(X; K(\pi, n))$ with $H^n(X; \pi)$:

$$(3.1) \qquad \cdots \to \pi(X; {}^1\mathfrak{P}) \xrightarrow{({}^1p)_\#} H^{n-1}(X; \pi) \xrightarrow{{}^1\theta} H^{n'}(X; \pi')$$
$$\xrightarrow{i_\#} \pi(X; \mathfrak{P}) \xrightarrow{p_\#} H^n(X; \pi) \xrightarrow{\theta} H^{n'+1}(X; \pi').$$

Let $h \in H^n(X; \pi)$ be such that $\theta(h) = 0$. Then by exactness of (3.1) there is a $v \in \pi(X; \mathfrak{P})$ such that $p_\#(v) = h$. Define $\Phi_v(h) = v^*(\phi) \in H^q(X; G)$ and $\Phi(h) = \{\Phi_v(h)\}$, i. e. $\Phi(h)$ is the collection of $\Phi_v(h)$ for all v such that $p_\#(v) = h$. Φ is the secondary operation determined by ϕ.

To define an $m+1$-ary operation now, let $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$ let $\mathfrak{P}' = \mathfrak{P}(\pi, n; \pi', n', \theta; \pi'', n'', \theta')$, and in general, let

$$\mathfrak{P}^{(i)} = \mathfrak{P}(\pi, n; \pi', n', \theta; \cdots; \pi^{(i+1)}, n^{(i+1)}, \theta^{(i)}),$$

and let $\phi \in H^q(\mathfrak{P}^{(m-1)}; G)$. We have the exact couple described in [8], part of which is:

$$\begin{tikzcd}
H^{n^{(m)}}(X;\pi^{(m)}) \arrow[r, "i_{\#}^{(m-1)}"] & \pi(X;\mathfrak{P}^{(m-1)}) \arrow[r, "\phi_{\#}"] \arrow[d, "p_{\#}^{(m-1)}"'] & H^{q}(X;G) \\
H^{n^{(m-1)}}(X;\pi^{(m-1)}) \arrow[r, "i_{\#}^{(m-2)}"] & \pi(X;\mathfrak{P}^{(m-2)}) \arrow[r, "\theta_{\#}^{(m-1)}"] \arrow[d, "p_{\#}^{(m-2)}"'] & H^{n^{(m)}+1}(X;\pi^{(m)}) \\
H^{n^{(m-2)}}(X;\pi^{(m-2)}) \arrow[r, "i_{\#}^{(m-3)}"] & \pi(X;\mathfrak{P}^{(m-3)}) \arrow[r, "\theta_{\#}^{(m-2)}"] \arrow[d, "p_{\#}^{(m-3)}"'] & H^{n^{(m-1)}+1}(X;\pi^{(m-1)}) \\
 & \vdots \arrow[d, "p_{\#}'"'] & \\
H^{n'}(X;\pi') \arrow[r, "i_{\#}"] & \pi(X;\mathfrak{P}) \arrow[r, "\theta_{\#}^{(1)}"] \arrow[d, "p_{\#}"'] & H^{n''+1}(X;\pi'') \\
 & H^{n}(X;\pi) \arrow[r, "\theta"] & H^{n'+1}(X;\pi').
\end{tikzcd}$$

We recall that in this diagram, the sequences which begin at the far left, go one step to the right, one step down, and one step to the right, are exact. Furthermore, we note that if $\Theta^{(1)}$ is the secondary operation associated with $\theta^{(1)}$, then for any $h \in H^{n}(X;\pi)$ such that $\theta(h)=0$, $\Theta^{(1)}(h)$ is the collection $\{\theta_{\#}^{(1)}(v)\}$ for all $v \in \pi(X;\mathfrak{P})$ such that $p_{\#}(v)=h$. We assume inductively that i-ary operations have been defined for $1 \leqq i \leqq m$ and we denote by $\Theta^{(i)}$ the $(i+1)$-ary operation associated with $\theta^{(i)}$. We assume that $\Theta^{(i)}$ is defined for those elements $h \in H^{n}(X;\pi)$ such that $0 \in \Theta^{(i-1)}(h)$ and that in this case, $\Theta^{(i)}(h)$ is the collection $\{\theta_{\#}^{(i)}(v)\}$ for all $v \in \pi(X;\mathfrak{P}^{(i-1)})$ such that $p_{\#}\,p_{\#}' \cdots p_{\#}^{(i-1)}(v)=h$. There are such elements v because of the assumption that $0 \in \Theta^{(i-1)}(h)$. We now assume that $0 \in \Theta^{(m-1)}(h)$—note that this implies that $\Theta^{(i)}(h)$ is defined for $0 \leqq i \leqq m-1$—and define $\Phi(h) \subset H^{q}(X;G)$ to be the set of elements $\{\phi_{\#}(v)\}$ for all $v \in \pi(X;\mathfrak{P}^{(m-1)})$ such that

$$p_{\#}p_{\#}' \cdots p_{\#}^{(m-2)}p_{\#}^{(m-1)}(v)=h.$$

Returning to the case of secondary operations, let $\mathfrak{P}=\mathfrak{P}(\pi,n;\pi',n',\theta)$, let $\phi \in H^{q}(\mathfrak{P};G)$ and let $\theta'=i^{*}(\phi) \in H^{q}(\pi',n';G)$. We give a lemma now which will be used later:

LEMMA 3.2. *If $q<n+n'$, there is a unique element*

$${}^{-1}\theta' \in H^{q+1}(\pi',n'+1;G)$$

such that ${}^{1}({}^{-1}\theta')=\theta'$, and we have ${}^{-1}\theta'(\theta)=0 \in H^{q+1}(\pi,n;G)$.

Proof. The fact that there exists a ${}^{-1}\theta' \in H^{q+1}(\pi', n'+1; G)$ such that ${}^{1}({}^{-1}\theta') = \theta'$ follows immediately from the suspension theorem of Eilenberg-MacLane [3] because $q < n + n' \leqq 2n' - 1$.

Let τ denote the transgression in the fibre space $\mathfrak{P} \to K(\pi, n)$. Since $i^*(\phi) = \theta'$, we have that $\tau(\theta') = 0$ by the exact sequence in [2]. However, since $q < n + n'$, we have $\tau(\theta'(\iota')) = {}^{-1}\theta'(\tau(\iota'))$, where $\iota' \in H^{n'}(\pi', n'; \pi')$ is the basic class. Hence $0 = \tau(\theta'(\iota')) = {}^{-1}\theta'(\tau(\iota')) = {}^{-1}\theta'(\theta)$.

We now wish to study the algebraic nature of the sets $\Phi(h) = \{\Phi_v(h)\}$, where Φ is a secondary cohomology operation. We will consider a homotopy associative principal fibre space (E, p, B, F, μ, h) with B $(n-1)$-connected and F $(n'-1)$-connected $(n' > n)$. If $q < n + n'$, it follows from the Künneth theorem that

$$H^q(F \times E; G) \approx H^q(F; G) \otimes H^0(E) + H^0(F) \otimes H^q(E; G),$$

and we will identify these groups.

LEMMA 3.3. *If $\phi \in H^q(E; G)$ with $q < n + n'$, then*

$$\mu^*(\phi) = i^*(\phi) \otimes 1 + 1 \otimes \phi,$$

where $i\colon F \to E$ is the inclusion.

Proof. From the defintion of a principal fibre space, we have

$$m^* i^*(\phi) = (1 \times i)^* \mu^*(\phi),$$

and the standard argument shows

$$m^* i^*(\phi) = i^*(\phi) \otimes 1 + 1 \otimes i^*(\phi)$$

since $q < n + n' < 2n'$.

We can write

$$\mu^*(\phi) = \alpha \otimes 1 + 1 \otimes \beta,$$

and we then see that $\alpha = i^*(\phi)$ and $i^*(\beta) = i^*(\phi)$.

On the other hand, since our fibre space is homotopy associative, we have

$$(j \times 1)^* \mu^*(\phi) = \pi^*(\phi) = 1 \otimes \phi. \quad \text{(See end of § 1.)}$$

But

$$(j \times 1)^* (i^*(\phi) \otimes 1 + 1 \otimes \beta) = 1 \otimes \beta$$

and thus $\beta = \phi$.

THEOREM 3.4. *Let $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$ and let $\phi \in H^q(\mathfrak{P}; G)$ with $q < n + n'$. Let Φ be the secondary cohomology operation associated with ϕ. Let X be any space and let $h \in H^n(X; \pi)$ be such that $\theta(h) = 0 \in H^{n'+1}(X; \pi')$.*

Then

$$\Phi(h) \in H^q(X;G)/\theta' H^{n'}(X;\pi')$$

where $\theta' = i^*(\phi) \in H^q(\pi', n'; G)$.

Proof. If $v, v' \in \pi(X;\mathfrak{P})$ are such that $p_\#(v) = p_\#(v') = h$, then according to Lemma 1.2, there exists a $w \in H^{n'}(X;\pi')$ such that $\mu_\#(w,v) = v'$. It then follows from Lemma 1.3 and Lemma 3.3 that

$$\begin{aligned} v'^*(\phi) &= \mu_\#(w,v)^*(\phi) = (w,v)^*(\mu^*(\phi)) \\ &= (w,v)^*(i^*(\phi)\otimes 1 + 1\otimes\phi) \\ &= (w,v)^*(\theta'\otimes 1 + 1\otimes\phi) \\ &= w^*(\theta') \cup 1 + 1 \cup v^*(\phi) \\ &= \theta'(w) + v^*(\phi). \end{aligned}$$

Thus

$$v'^*(\phi) - v^*(\phi) = \theta'(w) \in \theta' H^{n'}(X;\pi'),$$

which shows that any two element of $\Phi(h)$ differ by an element of $\theta' H^{n'}(X;\pi')$, and since $q < n + n' < 2n'$, θ' is additive and hence $\theta' H^{n'}(X;\pi')$ is a subgroup of $H^q(X;G)$. Furthermore, any element $w \in H^{n'}(X;\pi')$ gives rise to an element $v' \in \pi(X;\mathfrak{P})$ such that

$$p_\#(v') = p_\#(v) = h \text{ and } v'(\phi) = v^*(\phi) + \theta'(w).$$

Suppose now that $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$ and $\phi \in H^{n+n'}(\mathfrak{P};G)$. It follows from the Künneth theorem that

$$\begin{aligned} H^{n+n'}(F\times\mathfrak{P};G) \approx H^{n+n'}(F;G)\otimes H^0(\mathfrak{P}) \\ + H^0(F)\otimes H^{n+n'}(\mathfrak{P};G) + H^{n'}(F;H^n(\mathfrak{P};G)), \end{aligned}$$

where we have written F for $K(\pi', n')$. Now

$$H^{n'}(F;H^n(\mathfrak{P};G)) \approx \mathrm{Hom}(\pi';\mathrm{Hom}(\pi;G)) \approx \mathrm{Hom}(\pi'\otimes\pi;G).$$

Let $\mathfrak{P}' = \mathfrak{P}(\pi, n; \pi', n', \theta; G, n+n'-1, \phi)$. There is a Whitehead product homomorphism $\pi_{n'}(\mathfrak{P}')\otimes\pi_n(\mathfrak{P}') \to \pi_{n+n'-1}(\mathfrak{P}')$ which is an element $W \in \mathrm{Hom}(\pi'\otimes\&;G)$.

LEMMA 3.5.

$$\mu^*(\phi) = i^*(\phi)\otimes 1 + 1\otimes\phi + W.$$

Proof. For any space X and group G, we have a natural epimorphism $H^n(X;G) \to \mathrm{Hom}(H_n(X);G)$ carrying an element h into $h\vdash$. J. P. Meyer [18] has proved the following result: Let $\alpha \in \pi_{n'}(\mathfrak{P}')$, $\beta \in \pi_n(\mathfrak{P}')$, correspond to

$$\bar{\alpha} \in H_{n'}(\pi', n'; Z) \approx \pi_{n'}(K(\pi', n')) \approx \pi_{n'}(\mathfrak{P}) \approx \pi_{n'}(\mathfrak{P}')$$

and

$$\bar{\beta} \in H_n(\mathfrak{P}; Z) \approx H_n(\pi, n; Z) \approx \pi_n(K(\pi, n)) \approx \pi_n(\mathfrak{P}) \approx \pi_n(\mathfrak{P}')$$

respectively. We have the generalized Pontrjagin product $\bar{\alpha} * \bar{\beta} = \mu_*(\bar{\alpha} \times \bar{\beta}) \in H_{n+n'}(\mathfrak{P})$, where $\mu\colon K(\pi', n') \times \mathfrak{P} \to \mathfrak{P}$ is the multiplication. Then

$$\phi \vdash (\bar{\alpha} * \bar{\beta}) = [\alpha, \beta]$$

the Whitehead product of α and β.

The proof of Lemma 3.3 shows that the components of $\mu^*(\phi)$ in the first two terms of the direct sum decomposition are those indicated and we have only to identify the term in $H^{n'}(F; H^n(\mathfrak{P}; G))$. We have the diagram

$$\begin{tikzcd}
H_{n'}(F) \otimes H_n(\mathfrak{P}) \arrow[r, "P"] \arrow[dr] & H_{n+n'}(\mathfrak{P}) \arrow[r, "\phi\vdash"] & G \\
& H_{n+n'}(F \times \mathfrak{P}) \arrow[u, "\mu_*"] \arrow[ur, "\mu^*(\phi)\vdash"'] &
\end{tikzcd}$$

in which the unlabelled arrow denotes the cross-product, P denotes the Pontrjagin product, the left triangle is commutative by definition of P and the right one is commutative by naturality.

Now identifying $H_{n'}(F) \otimes H_n(\mathfrak{P})$ with $\pi' \otimes \pi$, the result of Meyer quoted above shows that going across the top line of our diagram is just W. It follows that

$$\begin{aligned} W(\bar{\alpha} \otimes \bar{\beta}) = \mu^*(\phi) \vdash (\bar{\alpha} \times \bar{\beta}) &= (i^*(\phi) \otimes 1 + 1 \otimes \phi + \chi) \vdash (\bar{\alpha} \times \bar{\beta}) \\ &= \chi(\bar{\alpha} \times \bar{\beta}), \end{aligned}$$

where χ is the component of $\mu^*(\phi)$ in $H^{n'}(F; H^n(\mathfrak{P}; G))$. It follows that $\chi = W$. (We have identified $H_{n'}(F) \otimes H_n(\mathfrak{P})$ as a direct summand of $H_{n+n'}(F \times \mathfrak{P})$ under the croos-product map.)

THEOREM 3.6.[2] *Let $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$ and let $\phi \in H^{n+n'}(\mathfrak{P}; G)$. Let X be any space and let $h \in H^n(X; \pi)$ be such that $\theta(h) = 0 \in H^{n'+1}(X; \pi')$. Then*

$$\Phi(h) \in H^{n+n'}(X; G)/[\theta' + h \cup] H^{n'}(X; \pi'),$$

where $\theta' = i^*(\phi)$ and where the cup-product is relative to the Whitehead product pairing W in $\mathfrak{P}' = \mathfrak{P}(\pi, n; \pi', n', \theta; G, n + n' - 1, \phi)$.

[2] This theorem has also been obtained by M. G. Barratt and by J. P. Meyer.

Proof. As before, we consider $v, v' \in \pi(X; \mathfrak{P})$ such that $p_{\#}(v) = p_{\#}(v') = h$, and $w \in H^{n'}(X; \pi')$ such that $\mu_{\#}(w, v) = v'$. We then find

$$v'^*(\phi) = (w, v)^*(\theta' \otimes 1 + 1 \otimes \phi + W)$$

There is a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(\pi', \pi') \otimes \mathrm{Hom}(\pi, \pi) \arrow[rr, "W_{\#}"] \arrow[d, "\approx"] & & \mathrm{Hom}(\pi' \otimes \pi; G) \arrow[dd] \\
H^{n'}(F; \pi') \otimes H^{n}(\mathfrak{P}; \pi) \arrow[d] & & \\
H^{n'}(F \times \mathfrak{P}; \pi') \otimes H^{n}(F \times \mathfrak{P}; \pi) \arrow[rr] & & H^{n+n'}(F \times \mathfrak{P}; G),
\end{tikzcd}$$

where the bottom line is the cup product relative to W. Then if $\iota \in H^{n}(\mathfrak{P}; \pi)$ and $\iota' \in H^{n'}(F; \pi')$ are the basic classes which we identify with their images in the cohomology of $F \times \mathfrak{P}$, and if $1' \in \mathrm{Hom}(\pi', \pi')$ and $1 \in \mathrm{Hom}(\pi, \pi)$ are the identity homomorphisms, then $1' \otimes 1$ corresponds to $\iota' \otimes \iota$. But $W_{\#}(1' \otimes 1) = W$ and hence W corresponds to $\iota' \cup \iota$. Thus

$$(w, v)^*(W) = (w, v)^*(\iota' \cup \iota) = w \cup v^*(\iota) = w \cup h.$$

Now as before,

$$v'^*(\phi) - v^*(\phi) = \theta'(w) + w \cup h \in [\theta' + h \cup] H^{n'}(X; \pi')$$

which is a subgroup since again $n + n' < 2n'$, and so θ' is additive. Furthermore, any element $w \in H^{n'}(X; \pi')$ gives rise to an element $v' \in \pi(X; \mathfrak{P})$ such that $p_{\#}(v') = p_{\#}(v) = h$ and $v'^*(\phi) = v^*(\phi) + \theta'(w) + w \cup h$.

4. Cohomology operations and obstructions. For simplicity, we treat only the case of secondary operations. The general case is similiar but more complicated. Let $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$, let $\phi \in H^{n''+1}(\mathfrak{P}; \pi'')$ and let $\mathfrak{P}' = \mathfrak{P}(\pi, n; \pi', n', \theta; \pi'', n'', \phi)$. Let X be any complex, X^i its i-skeleton, and consider a map $f\colon X^n \to \mathfrak{P}$ which can be extended to X^{n+1}, and hence to $X^{n'}$. Now let $\iota \in H^n(\mathfrak{P}; \pi)$ be the basic class. The obstruction to extending f to a map $X^{n'+1} \to \mathfrak{P}$ is just $\theta(f^*(\iota))$. If we assume that $\theta(f^*\iota) = 0$, we can find extensions $f'\colon X^{n'+1} \to \mathfrak{P}$ of f and hence extensions $f'\colon X^{n''} \to \mathfrak{P}$ of f. For each such extension, there is defined an obstruction cocycle in $Z^{n''+1}(X; \pi'')$ and hence an obstruction class in $H^{n''+1}(X; \pi'')$. This class is not uniquely determined by f, but depends on the choice of an intermediate extension.

It is one of the classes $\Phi_v(f^*\iota)$ in § 3. The set $\Phi(f^*\iota)$ is the collection of all such obstruction classes for all possible intermediate extensions of f.

Chapter II. The Main Theorems.

5. Functional cohomology operations. In this section, we recall two definitions of functional primary cohomology operations and prove a theorem showing that they are the same.

Let $f\colon L \to K$ and let $\theta \in H^{n'+1}(\pi, n; \pi')$. Assuming f is an inclusion, we consider the following commutative diagram, where each row is the exact sequence of the pair (K, L):

$$\begin{tikzcd}
 & H^{n-1}(L;\pi) \arrow[r, "\delta"] \arrow[d, "{}^1\theta"] & H^n(K,L;\pi) \arrow[r, "j^*"] \arrow[d, "\theta"] & H^n(K;\pi) \arrow[r, "f^*"] \arrow[d, "\theta"] & H^n(L;\pi) \\
H^{n'}(K;\pi') \arrow[r, "f^*"] & H^{n'}(L;\pi') \arrow[r, "\delta"] & H^{n'+1}(K,L;\pi') \arrow[r, "j^*"] & H^{n'+1}(K;\pi'). &
\end{tikzcd}$$

Let $h \in H^n(K;\pi)$ be such that $\theta(h) = 0$ and $f^*(h) = 0$. By exactness, there exists an element $v \in H^n(K, L; \pi)$ such that $j^*(v) = h$. Since $j^*\theta(v) = \theta j^*(v) = \theta(h) = 0$, there exists an element $x \in H^{n'}(L;\pi')$ such that $\delta(x) = \pi(v)$. The set of all x such that $\delta(x) = \theta(v)$ with $j^*(v) = h$ is defined to be $\theta_f(h)$. in case θ is an additive cohomology operation, it is easy to see that $\theta_f(h)$ is a coset of $f^*(H^{n'}(K;\pi') + {}^1\theta(H^{n-1}(L;\tau)) \subset H^{n'}(L;\pi')$, and hence can be considered as an element in $H^{n'}(L;\pi')/\mathrm{Im}\, f^* + \mathrm{Im}\, {}^1\theta$.[3]

A second definition of functional primary cohomology operations is obtained by considering the following commutative diagram. Here the rows are exact sequences 3.1 applied to the fibration of the Postnikov space $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$.

$$\begin{tikzcd}
 & H^{n'}(K;\pi') \arrow[r, "i_\#"] \arrow[d, "f^*"] & \pi(K;\mathfrak{P}) \arrow[r, "p_\#"] \arrow[d, "f^\#"] & H^n(K;\pi) \arrow[r, "\theta"] \arrow[d, "f^*"] & H^{n'+1}(K;\pi') \\
H^{n-1}(L;\pi) \arrow[r, "{}^1\theta"] & H^{n'}(L;\pi') \arrow[r, "i_\#"] & \pi(L;\mathfrak{P}) \arrow[r, "p_\#"] & H(L;\pi). &
\end{tikzcd}$$

Let $h \in H^n(K;\pi)$ be such that $f^*(h) = 0$ and $\theta(h) = 0$. As before, define $\bar\theta_f(h)$ to be the set of elements $x \in H^{n'}(L;\tau')$ such that $i_\#(x) = f^\#(v)$ with $p_\#(v) = h$. Again $\bar\theta_f(h)$ can be considered an element of

$$H^{n'}(L;\pi')/\mathrm{Im}\, {}^1\theta + \mathrm{Im}\, f^*.$$

[3] It is shown in [9] that this is true even when θ is not additive.

In [8] it is shown that there is an automorphism λ of a subgroup of $H^{n'}(L;\pi')/\mathrm{Im}\,{}^1\theta + \mathrm{Im}\,f^*$ such that $\lambda\tilde{\theta}_f(h) = \theta_f(h)$ for all $u \in \mathrm{Ker}\,f^* \cap \mathrm{Ker}\,\theta$. We now strengthen this result.

THEOREM 5.1. $\bar{\theta}_f(h) = \theta_f(h)$.

Proof. This proof and most of the proofs to follow will use the method of universal examples. In this proof, we will show how the general result follows from the result in a universal example; later, these details will be omitted.

Special case. Let $L = K(\pi', n')$, $K = \mathfrak{P}$, $f = i\colon K(\pi', n') \to \mathfrak{P}$ be the inclusion of the fibre in the total space of the fibre space $p\colon \mathfrak{P} \to K(\pi, n)$, and let $h = [p] \in H^n(\mathfrak{P};\pi)$. Clearly $i^*([p]) = 0$ and $\theta([p]) = 0$. In the second definition, we may take $v = [1]$ because $p_\#([1]) = [p]$. Also, $i^\#([1]) = [i] = i_\#(\iota')$, where $\iota' \in H^{n'}(\pi', n';\pi') \approx \pi(K(\pi', n'); K(\pi', n'))$ denotes the cohomology class corresponding to the identity map. Hence, $\bar{\theta}_i([p]) = \{\iota'\} \in H^{n'}(\pi', n';\pi')/\mathrm{Im}\,i^* + \mathrm{Im}\,{}^1\theta$. It is well-known that if $r < n + n'$, then $p_1{}^*\colon H^r(\pi, n; G) \to H^r(\mathfrak{P}, K(\pi', n'); G)$ is an isomorphism and the following diagram is commutative:

$$\begin{tikzcd}
H^{r-1}(K(\pi', n'); G) \arrow[r, "\tau"] \arrow[dr, "\delta"'] & H^r(\pi, n; G) \arrow[r, "p^*"] \arrow[d, "p_1{}^*"] & H^r(\mathfrak{P}; G) \\
 & H^r(\mathfrak{P}, K(\pi', n'); G), \arrow[ur, "j^*"'] &
\end{tikzcd}$$

where τ is the transgression homomorphism [2]. Since $n' + 1 < n + n'$ and $n < n + n'$, the diagram defining $\theta_i([p])$ may be replaced by the following diagram.

$$\begin{tikzcd}
 & H^{n-1}(\pi', n';\pi) \arrow[r, "\tau"] \arrow[d, "{}^1\theta"] & H^n(\pi, n;\pi) \arrow[r, "p^*"] \arrow[d, "\theta"] & H^n(\mathfrak{P};\pi) \arrow[r, "i^*"] \arrow[d, "\theta"] & H^n(\pi', n';\pi) \\
H^{n'}(\mathfrak{P};\pi') \arrow[r, "i^*"] & H^{n'}(\pi', n';\pi') \arrow[r, "\tau"] & H^{n'+1}(\pi, n';\pi') \arrow[r, "p^*"] & H^{n'+1}(\mathfrak{P};\pi'). &
\end{tikzcd}$$

As above, let $\iota \in H^n(\pi, n;\pi)$ be the fundamental class. Then $p^*(\iota) = [p]$, and by definition of $\mathfrak{P}$, $\theta(\iota) = \tau(\iota')$. Hence

$$\theta_i([p]) = \{\iota'\} = \bar{\theta}_i([p]) \in H^{n'}(\pi', n;\pi')/\mathrm{Im}\,i^* + \mathrm{Im}\,{}^1\theta.$$

General Case. Let $f\colon L \to K$, $h \in H^n(K;\pi)$, $\theta(h) = 0$, and $f^*(h) = 0$. Let $\chi(h)\colon K \to K(\pi, n)$ represent h. Since $\theta(h) = 0$, there exists a map

$\bar{\chi}(h) : K \to \mathfrak{P}$ such that $p_{\#}[\bar{\chi}(h)] = [\chi(h)] = h$. Since $f^*(h) = 0$, there exists a map $\tilde{\chi}(h) : L \to K(\pi', n')$ such that the following diagram is commutative up to homotopy:

$$\begin{tikzcd} L \arrow[r, "\tilde{\chi}(h)"] \arrow[d, "f"'] & K(\pi', n') \arrow[d, "i"] \\ K \arrow[r, "\bar{\chi}(h)"] & \mathfrak{P}. \end{tikzcd}$$

By an obvious naturality condition for functional cohomology operations, we have

$$\begin{aligned} \theta_f(h) &= \theta_f(\chi(h)^*([p]) = \tilde{\chi}(h)^*\theta_i([p]) \\ &= \tilde{\chi}(h)^*\bar{\theta}_i([p]) = \bar{\theta}_f(\bar{\chi}(h)^*([p])) = \bar{\theta}_f(h). \end{aligned}$$

6. The two formulas. In this section, we state and prove our two formulas relating secondary cohomology operations and primary cohomology operations. To avoid technical complications, we restrict ourselves in this section to stable secondary cohomology operations of a single variable. More general situations will be discussed in Sections 7 and 8.

As in Section 3, let $\theta \in H^{n'+1}(\pi, n; \pi')$, $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n'; \theta)$, and let $\phi \in H^q(\mathfrak{P}; G)$ define the secondary cohomology operation Φ. Let $\theta'(\iota') = i^*(\phi) \in H^q(\pi', n'; G)$. We will assume that $q < n + n'$ throughout this section.

THEOREM 6.1. *Let $f: L \to K$ and $h \in H^n(K; \pi)$ be such that $f^*(h) = 0$ and $\theta(h) = 0$. Then*[4]

$$f^*\Phi(h) = \theta'(\theta_f(h)) \in H^q(L; G)/\theta' f^*(H^{n'}(K; \pi')).$$

Proof. We give a proof in the universal example. The general case then follows as in the proof of Theorem 5.1. Let $L = K(\pi', n')$, $K = \mathfrak{P}$, $h = [p]$, and $f = i$. Since $p_{\#}[1] = [p]$, $\Phi([p]) = \{\phi_{\#}([1])\} = \{\phi\}$. However, as in the proof of Theorem 5.1, $\theta_i([p]) = \{\iota'\}$, and hence $\theta'(\theta_i([p]) = \theta'\{\iota'\} = i^*\Phi([p])$. To complete the proof, we must show that both sides are well-defined in general. According to Theorem 3.4, under the assumption $q < n + n'$, $\Phi(h) \in H^q(K; G)/\theta'(H^{n'}(K; \pi'))$. Hence

$$f^*\Phi(h) \in H^q(L; G)/\theta' f^*(H^{n'}(K; \pi')).$$

[4] Special cases of this formula were known to Shimada [12] and Stein [13].

The right hand side is defined modulo

$$\theta'(f^*(H^{n'}(K;\pi')) + {}^1\theta(H^{n-1}(L;\pi)) = \theta' f^*(H^{n'}(K;\pi'))$$

because $\theta'{}^1\theta = 0$ by Lemma 3.2.

Remark. Since Φ is natural, under the hypothesis of Theorem 6.1, we have $f^*\Phi(h) = \Phi(f^*(h)) = \Phi(0) = 0$. Here $0 \in H^q(L;G)/\theta'(H^{n'}(L;\pi'))$. Our theorem gives more delicate information as we factor out by the smaller subgroup $\theta' f^*(H^{n'}(K;\pi'))$ and show that $f^*\Phi(h)$ is the image under θ' of a particular element, $\theta_f(h)$.

Before stating our second formula, we prove the following lemma.

LEMMA 6.2. *Let $p: E \to B$ be a fibre space with fibre F and let $i: F \to E$ be the inclusion. Let $h \in H^{n'+1}(B;\pi')$ be such that $\tau(v) = h$, where $v \in H^{n'}(F;\pi')$ and τ is the transgression. Let $\psi \in H^{q+1}(\pi', n'+1; G)$ be such that $\psi(h) = 0$. Then*

$$i^*((\psi_p)(h)) = {}^1\psi(v) \in H^q(F;G)/{}^1\psi i^*(H^{n'}(E;\pi')).$$

Proof. Let $\chi(h): B \to K(\pi', n'+1)$ represent h. Since $\psi(h) = 0$, there exist a map $\tilde{\chi}(h): B \to \mathfrak{P}(\pi', n'+1; G, q, \psi) = \mathfrak{P}'$ such that $p'_{\#}(\tilde{\chi}(h)) = [\chi(h)] = h$, where $p': \mathfrak{P}' \to K(\pi', n'+1)$. Since $p^*(h) = 0$, there exists a map $\bar{\chi}(h): E \to K(G,q)$ such that the following diagram is commutative up to homotopy:

$$\begin{array}{ccc} E & \xrightarrow{\bar{\chi}(h)} & K(G,q) \\ \downarrow p & & \downarrow i' \\ B & \xrightarrow{\tilde{\chi}(h)} & \mathfrak{P}' \end{array}$$

We may assume that $i': K(G,q) \to \mathfrak{P}'$ is a fibre map and that $\bar{\chi}(h)$ is a fibre preserving map. Hence $\bar{\chi}(h) \mid F: F \to K(\pi', n')$ and $(\bar{\chi}(h) \mid F)^*(\iota') = \bar{v}$ is such that $\tau(\bar{v}) = \tau(\bar{\chi}(h) \mid F)^*(\iota') = \bar{\chi}(h)^*(\tau(\iota')) = \bar{\chi}(h)^*(\iota'_{n'+1}) = h$. Moreover, because $\bar{v} - v = i^*(x)$ for some $x \in H^{n'}(E;\pi')$,

$${}^1\psi(\bar{v}) = {}^1\psi(v) \in H^q(F;G)/\mathrm{Im}\,{}^1\psi i^*(H^{n'}(E;\pi')),$$

we need only prove our lemma for $\bar{v}$. Hence by naturality, it is sufficient to prove the lemma for the fibre space $i': K(G,q) \to \mathfrak{P}'$. As in the proof of Theorem 5.1, $(\psi)_{i'}([p]) = \iota''$, and since $i'': K(\pi', n') \to K(G,q)$, the inclusion of the fibre in the fibre space $i': K(G,q) \to \mathfrak{P}'$, is the loop functor applied to $\psi: K(\pi', n'+1) \to K(G, q+1)$, we have that $(i'')^*(\iota'') = {}^1\psi(\iota')$ and our lemma is proved.

We now prove our second formula. As above, let $\theta \in H^{n'+1}(\pi, n; \pi')$, $\mathfrak{P} = \mathfrak{P}(\pi, n; \pi', n', \theta)$, and let $\phi \in H^q(\mathfrak{P}; G)$ define the secondary operation Φ. Let $\theta'(\iota') = i^*(\phi) \in H^q(\pi', n'; G)$. Because $q < n + n'$, $\theta' = {}^1\psi$, where $\psi \in H^{q+1}(\pi', n' + 1; G)$.

THEOREM 6.3. *Let $f\colon L \to K$ and $h \in H^n(K; \pi)$ be such that $f^*\theta(h) = 0$. Then*

$$\Phi(f^*(h)) = \psi_f(\theta(h)) \in H^q(L; G)/f^*(H^q(K; G)) + \theta'(H^{n'}(L; \pi')).$$

Proof. We give this proof in the universal example. Let $L = \mathfrak{P}$, $K = K(\pi, n)$, $f = p$, and $h = \iota$. Then $\Phi(p^*(\iota)) = \phi$. By Lemma 6.2, with $h = \theta(\iota)$ we have $i^*((\psi)_p(\theta(\iota))) = \theta'(\iota') = i^*(\phi)$. However, under the dimensional restriction $q < n + n'$, an element in $H^q(\mathfrak{P}; G)$ is determined, modulo $p^*(H^q(\pi, n; G))$, by its image under i^*. Hence $(\psi)_p(\theta(\iota)) = \phi = \Phi(p^*(\iota)) \in H^q(\mathfrak{P}; G)/p^*(H^q(\pi, n; G)) + \theta'(H^{n'}(\mathfrak{P}; \pi'))$. To pass to the general case, it only has to be noted that both sides are well-defined.

Remark. The formulas in Theorems 6.1 and 6.3 are dual to each other. Notice that in Theorem 6.1, $h \in \operatorname{Ker} f^* \cap \operatorname{Ker} \theta$ and the values are in Coker $f^*\theta'$, while in Theorem 6.3, $h \in \operatorname{Ker} f^*\theta$ and the values are in Coker $(f^* + \theta')$. We hope to make this duality more precise and give some applications in a later paper.

7. A non-stable case. In this section, we generalize the formulas of the preceding section to some secondary cohomology operations where $q \geqq n + n'$. An example of this section will be discussed in detail in Section 10.

The condition $q < n + n'$ was used in the proof of Theorem 6.1 only to show that both sides of the formula were well-defined. Let $L(\phi, h)$ be the subgroup generated by all differences $\Phi_v(h) - \Phi_{v'}(h)$ for $p_\#(v) = p_\#(v') = h$. Then $\Phi(h)$ can be considered as an element of $H^q(K; G)/L(\phi, h)$ for $h \in H^n(K; \pi)$ with $\theta(h) = 0$. The proof of the following theorem is the same as that of Theorem 6.1.

THEOREM 7.1. *Let $f\colon L \to K$ and $h \in H^n(K; \pi)$ be such that $f^*(h) = 0$ and $\theta(h) = 0$. Assume that θ' is additive. Then*

$$f^*\Phi(h) = \theta'(\theta_f(h)) \in H^q(L; G)/f^*(L(\phi, h) + \theta' f^*(H^{n'}(K; \theta'))$$
$$+ \theta'^1\theta(H^{n-1}(L; \pi)).$$

We now discuss the case $q = n + n'$ for Theorem 6.3. Let $\theta \in H^{n'+1}(\pi, n; \pi')$. Assume that there exists an element $\phi \in H^q(\mathfrak{P}; G)$ such that $\theta' = i^*(\phi) = {}^1\psi$,

where $\psi \in H^{q+1}(\pi', n'+1; G)$ is such that $\psi(\theta) = \iota \cup \theta \in H^{q+1}(\pi, n; G)$ and the cup product is with respect to the Whitehead product pairing $\pi \otimes \pi' \to G$ (see Theorem 3.6).

THEOREM 7.2. *Let $f\colon L \to K$ and $h \in H^n(K;\pi)$ be such that $f^*\theta(h) = 0$. Then*

$$\Phi(f^*(h)) = (\psi - h \cup)_f(\theta(h)) \in H^q(L;G)/f^*(H^q(K;G)) + (\theta' - f^*(h) \cup)(H^{n'}(L;\pi')).$$

Before giving the proof of this theorem, we must discuss the definition of $(\psi - h \cup)_f$; it will be analogous to the second definition in Section 5.

Let $f\colon L \to K$, $h \in H^n(K;\pi)$, $v \in H^{n'+1}(K;\pi')$, and $\psi \in H^{q+1}(\pi', n'+1; G)$ be such that $f^*(v) = 0$ and $\psi(v) = h \cup v$. To define

$$(\psi - h \cup)_f(v) \in H^q(L;G)/f^*(H^q(K;G)) + ({}^1\psi - f^*(h) \cup)(H^{n'}(L;\pi')),$$

we study the universal example. Let

$$K = \mathfrak{P}(\pi, n; \pi', n'+1, 0;\, G, q, \psi(\iota') - \iota \cup \iota') = \bar{\mathfrak{P}},$$

let $L = \mathfrak{P}(\pi, n; \pi', n'+1, 0; G, q, \psi(\iota') - \iota \cup \iota'; \pi', n', \iota') = \mathfrak{P}'$, and let $p\colon \mathfrak{P}' \to \bar{\mathfrak{P}}$ be the fibre map. Consider the spectral sequence of this fibring. The element $\iota \otimes \iota' \in E_2^{n,n'}$ kills the element $\iota \cup \iota' = \psi(\iota') \in E_2^{n+n'+1,0}$ because $d^{n'+1}(\iota \otimes {}^1\iota') = \iota \cup \iota'$. Hence all (d^r)'s are 0 on the element ${}^1\psi({}^1\iota') \in E_2^{0,n+n'}$. This element gives rise to an element in $H^{n+n'}(\mathfrak{P}';G)$, defined modulo $p^*H^q(\bar{\mathfrak{P}};G)$, which we define to be $(\psi - \iota \cup)_p(\iota')$. The general definition is obtained by mapping into the universal example.

The proof of Lemma 6.2 now generalizes to a proof of the following lemma:

LEMMA 7.3. *Let $p\colon E \to B$ be a fibre space with fibre F and let $i\colon F \to E$ be the inclusion. Let $h \in H^n(B;\pi)$, $v \in H^{n'+1}(B;\pi')$, and $\psi \in H^{q+1}(\pi', n'+1; G)$ be such that $\psi(v) = h \cup v$ and $\tau(w) = v$, where $w \in H^{n'}(F;\pi')$. Then*

$$i^*(\psi - h \cup)_p(v) = {}^1\psi(w) \in H^q(F;G)/{}^1\psi i^*(H^{n'}(E;\pi')).$$

With this lemma, the proof of Theorem 6.3 easily generalizes to a proof of Theorem 7.2.

8. Cohomology operations on several variables. Our two formulas have analogs for secondary cohomology operations on more than one variable. In this section, we give the analog for the Massey triple product [15].

Let $u \in H^p(K)$, $v \in H^q(K)$, and $w \in H^r(K)$, where the coefficients are

2

in a commutative ring with unit. If $u \cup v = 0$ and $v \cup w = 0$, then the triple product $\langle u, v, w\rangle \in H^{p+q+r-1}(K)/u \cup H^{q+r-1}(K) + H^{p+q-1}(K) \cup v$ is defined as follows. Let $\bar{u}$, $\bar{v}$, and $\bar{w}$ be cocycles representing u, v, and w respectively. Let $\delta a = \bar{u} \cup \bar{v}$, $\delta b = \bar{v} \cup \bar{w}$. Then a representative of $\langle u, v, w\rangle$ is $a \cup \bar{w} + (-1)^{p+1}\bar{u} \cup b$.

We now define left and right functional cup products. Let $f\colon L \to K$, $u \in H^p(K)$, and $v \in H^q(K)$. If $u \cup v = 0$ and $f^*(u) = 0$, then

$$u \overset{L}{\underset{f}{\cup}} v \in H^{p+q-1}(L)/f^*H^{p+q-1}(K) + H^{p-1}(L) \cup f^*(v)$$

is defined as follows: Let $\delta c = f^\#(\bar{u})$, where $f^\#$ is the cochain map induced by f. Then a representative of $u \overset{L}{\underset{f}{\cup}} v$ is $f^\#(a) - c \cup f^\#(\bar{v})$. Also, if $u \cup v = 0$ and $f^*(v) = 0$, then $u \overset{R}{\underset{f}{\cup}} v \in H^{p+q-1}(L)/f^*(H^{p+q-1}(K)) + f^*(u) \cup H^{q-1}(L)$ is defined as follows: Let $\delta d = f^\#(\bar{v})$. Then a representative of $u \overset{R}{\underset{f}{\cup}} v$ is $f^\#(a) + (-1)^{p+1} f^\#(\bar{u}) \cup d$.

The analog of Theorem 6.1 is the following theorem.

THEOREM 8.1. *Let $u \in H^p(K)$, $v \in H^q(K)$, $w \in H^r(K)$, and $f\colon L \to K$ be such that $f^*(u) = 0$, $u \cup v = 0$, and $v \cup w = 0$. Then*[5]

$$f^*\langle u, v, w\rangle = (u \overset{L}{\underset{f}{\cup}} v) \cup f^*(w) \in H^{p+q+r-1}(L)/f^*(H^{q+r-1}(K) \cup w).$$

Proof. Let $\delta a = \bar{u} \cup \bar{v}$, $\delta b = \bar{v} \cup \bar{w}$, *and* $\delta c = f^\#(\bar{u})$. Then $f^*\langle u, v, w\rangle$ has as a representative

$$\begin{aligned} &f^\#(a) \cup f^\#(\bar{w}) + (-1)^{p+1} f^\#(\bar{u}) \cup f^\#(b) \\ &\qquad = f^\#(a) \cup f^\#(\bar{w}) + (-1)^{p+1} \delta c \cup f^\#(b). \end{aligned}$$

On the other hand, $(u \overset{L}{\underset{f}{\cup}} v) \cup f^*(w)$ has a representative

$$f^\#(a) \cup f^\#(\bar{w}) - c \cup f^\#(\bar{v}) \cup f^\#(\bar{w}) = f^\#(a) \cup f^\#(\bar{w}) - c \cup \delta f^\#(b).$$

However, $\delta(c \cup f^\#(b)) = \delta c \cup f^\#(b) + (-1)^{p-1} c \cup \delta f^\#(b)$, and hence the representatives of $f^*\langle u, v, w\rangle$ and $(u \overset{L}{\underset{f}{\cup}} v) \cup f^*(w)$ differ by $\delta((-1)^{p+1} c \cup f^\#(b))$.

The analog of Theorem 6.3 is the following theorem.

THEOREM 8.2. *Let $u \in H^p(K)$, $v \in H^q(K)$, $w \in H^r(K)$, and $f\colon L \to K$ be such that $f^*(u \cup v) = 0$, $f^*(v \cup w) = 0$, and $u \cup v \cup w = 0$. Then*

[5] Formulas similar to this appear in [15].

$$\langle f^*(u), f^*(v), f^*(w)\rangle$$
$$= u \overset{R}{\underset{f}{\cup}} (v \cup w) - (u \cup v) \overset{L}{\underset{f}{\cup}} w \in H^{p+q+r-1}(L)/f^*(u) \cup H^{q+r-1}(L)$$
$$+ H^{p+q-1}(L) \cup f^*(w) + f^*(H^{p+q+r-1}(K)).$$

Proof. Let $\delta a = f^{\#}(\bar{u} \cup \bar{v}) = f^{\#}(\bar{u}) \cup f^{\#}(\bar{v})$, $\delta b = f^{\#}(\bar{v} \cup \bar{w})$, and $\delta c = \bar{u} \cup \bar{v} \cup \bar{w}$. Then $\langle f^*(u), f^*(v), f^*(w)\rangle$ has as a representative

$$(-1)^{p+1} f^{\#}(\bar{u}) \cup b + a \cup f^{\#}(\bar{w}).$$

However, $u \overset{R}{\underset{f}{\cup}} (v \cup w) - (u \cup v) \overset{L}{\underset{f}{\cup}} w$ has as a representative

$$f^{\#}(c) + (-1)^{p+1} f^{\#}(\bar{u}) \cup b - (f^{\#}(c) - a \cup f^{\#}(\bar{w}))$$
$$= (-1)^{p+1} f^{\#}(\bar{u}) \cup b + a \cup f^{\#}(\bar{w}).$$

The generalizations of these formulas to n-tuple products are straightforward and are left to the reader.

Chapter III. Applications.

9. The Adem operation. ([1]) Let $\mathfrak{P}_n = \mathfrak{P}(Z, n; Z_2, n+1, Sq^2\iota)$ with $n \geqq 4$. (Only a slight change is necessary to handle the case $n = 3$.) $\mathfrak{P}_n$ is a fibre space over $K(Z, n)$ with fibre $K(Z_2, n+1)$. We consider the mod 2 cohomology of $\mathfrak{P}_n$. Let $\iota \in H^n(Z, n; Z_2) \approx Z_2$ be the generator. Then $H^{n+1}(Z, n; Z_2) = 0$, $H^{n+2}(Z, n; Z_2) \approx Z_2$ generated by $Sq^2\iota$, $H^{n+3}(Z, n; Z_2) \approx Z_2$ generated by $Sq^3\iota$, and $H^{n+4}(Z, n; Z_2) \approx Z_2$ generated by $Sq^4\iota$. Similarly, if ι' generates $H^{n+1}(Z_2, n+1; Z_2) \approx Z_2$, then $H^{n+2}(Z_2, n+1; Z_2) \approx Z_2$ generated by $Sq^1\iota'$, $H^{n+3}(Z_2, n+1; Z_2) \approx Z_2$ generated by $Sq^2\iota'$. Furrthermore, we have $\tau(\iota') = Sq^2\iota$, and hence $\tau(Sq^1\iota') = Sq^1Sq^2\iota = Sq^3\iota$ and $\tau(Sq^2\iota') = Sq^2Sq^2\iota = Sq^3Sq^1\iota = 0$. It follows that $H^i(\mathfrak{P}_n; Z_2) = 0$ for $i < n$, $H^n(\mathfrak{P}_n; Z_2) \approx Z_2$ generated by $p^*\iota$, $H^{n+1}(\mathfrak{P}_n; Z_2) = 0$, $H^{n+2}(\mathfrak{P}_n; Z_2) = 0$, and $H^{n+3}(\mathfrak{P}_n; Z_2) \approx Z_2$ generated by an element ϕ_n such that $i^*(\phi_n) = Sq^2\iota' \in H^{n+3}(Z_2, n+1; Z_2)$. These results all follow from the exact sequence of Cartan-Serre [2]. ϕ_n gives rise to a secondary cohomology operation Φ_n which is defined, for any space X, on those elements $h \in H^n(X; Z)$ such that $Sq^2h = 0 \in H^{n+2}(X; Z)$, and since $n \geqq 3$, we can apply Theorem 3.4 to see that Φ_n takes its values in $H^{n+3}(X; Z_2)/Sq^2H^{n+1}(X; Z_2)$.

As the first application of our earlier results, we prove a formula which occurred in computations Peterson has made of homotopy groups of the unitary groups. The proof illustrates a useful way to apply our main

theorems to compute secondary cohomology operations. Namely, to compute a secondary operation Φ on a class h in a space X, construct a space Y and a map $f\colon Y\to X$ so that the induced cohomology map is a monomorphism in the dimension of $\Phi(h)$, and $f^*(h)=0$. Such a space can often be constructed as a fibre space over X with a $K(\pi,n)$ as fibre and h as k-invariant. Then apply Theorem 6.1.

THEOREM 9.1. *Let $\iota\in H^4(Z,4;Z)\approx Z$ be a generator and let δ^* be the Bockstein operator associated with the exact sequence $0\to Z\to Z\to Z_2\to 0$. Then*

$$\Phi_7(\delta^*Sq^2\iota)=0\in H^{10}(Z,4;Z_2).$$

Proof. We note first that $H^8(Z,4;Z_2)\approx Z_2$ is generated by ι^2 and that $Sq^2\iota^2=0$, so that $Sq^2H^8(Z,4;Z_2)=0$, and hence Φ_7 does take its values in $H^{10}(Z,4;Z_2)$ rather than in a quotient of this group.

Let $\mathfrak{P}=\mathfrak{P}(Z,4;Z,6,\delta^*Sq^2\iota)$, and let $f\colon\mathfrak{P}\to K(Z,4)$ be the fibre map. A straightforward calculation with the spectral sequence of f shows that $H^{10}(\mathfrak{P};Z_2)\approx Z_2+Z_2+Z_2$, and the generators are $f^*(\iota Sq^2\iota)$, $f^*(Sq^4Sq^2\iota)$, and an element α such that $i^*(\alpha)=Sq^4\iota'\in H^{10}(Z,6;Z_2)$, where $i\colon K(Z,6)\to\mathfrak{P}$ is the inclusion of the fibre, and ι' generates $H^6(Z,6;Z_2)$. Thus f^* is a monomorphism on $H^{10}(Z,4;Z_2)$. We apply Theorem 6.1 and find that

$$f^*\Phi_7(\delta^*Sq^2\iota)=Sq^2Sq^2{}_f\delta^*Sq^2\iota\in H^{10}(\mathfrak{P};Z_2)/Sq^2f^*H^8(Z,4;Z_2).$$

But $Sq^2f^*\iota^2=0$, so the relation holds in $H^{10}(\mathfrak{P};Z_2)$. Furthermore, $i^*(Sq^2Sq^2{}_f\delta^*Sq^2\iota)=Sq^2i^*(Sq^2{}_f\delta^*Sq^2\iota)\in Sq^2H^8(Z,6;Z_2)$. But $H^8(Z,6;Z_2)$ is generated by $Sq^2\iota'$ and $Sq^2Sq^2\iota'=Sq^3Sq^1\iota'=0$ so that $i^*(Sq^2Sq^2{}_f\delta^*Sq^2\iota)=0$. It follows that

$$Sq^2Sq^2{}_f\delta^*Sq^2\iota=a(f^*Sq^4Sq^2\iota)+b(f^*(\iota Sq^2\iota)),$$

where a and b are either 0 or 1.

Let $\mu=Sq^2{}_f\delta^*Sq^2\iota\in H^8(\mathfrak{P};Z_2)$. We have

$$Sq^2\mu(f^*\iota)=a(Sq^4Sq^2f^*\iota)+b(f^*\iota)(Sq^2f^*\iota).$$

Consider the space $S^2(CP(4))=S^4\cup e^6\cup e^8\cup e^{10}$, where $CP(4)$ is complex-projective 4-space. We have $Sq^2\{S^4\}=\{t^6\}$ and $Sq^4\{e^6\}=\{e^{10}\}$. Also $\{S^4\}\cup\{e^6\}=0$ since cup-products are zero in a suspension. It follows from Lemma 9.2 which we will prove below that $\mu\{S^4\}=0$. Thus

$$0=Sq^2\mu\{S^4\}=a\{e^{10}\}+0,$$

so that $a=0$.

Now let $Y = S^4 \cup e^6$, where e^6 is attached by $\eta_4 \neq 0 \in \pi_5(S^4)$. According to Theorem 1.2 of [5], there is a complex $X = Y \cup e^{10}$ such that $\{S^4\} \cup \{e^6\} = \{e^{10}\}$ if and only if $[\eta_4, \iota_4]$ is in the image of $(\eta_4)_* \colon \pi_8(S^5) \to \pi_8(S^4)$. On the other hand, we have, according to [14],

$$[\eta_4, \iota_4] = \alpha_4 \circ \eta_7 = \eta_4 \circ \nu_5 = (\eta_4)_*(\nu_5).$$

Hence there is a space X of the right type. We have $H^8(X; Z_2) = 0$, so that $\mu\{S^4\} = 0$. Thus $0 = Sq^2\mu\{S^4\} = 0 + b\{e^{10}\}$, so that $b = 0$.

This proves the theorem.

LEMMA 9.2. *The double suspension of* μ, ${}^2\mu = 0$ *as a cohomology operation.*

Proof. We consider the path space over $\mathfrak{P}$ with fibre ${}^1\mathfrak{P}$ and compute the mod 2 cohomology spectral sequence. It is easy to see that up to dimension 7 the only non-zero groups $H^i({}^1\mathfrak{P}; Z_2)$ are Z_2 in dimensions 3, 5, and 7 generated by classes whose transgressions are respectively ι, $Sq^2\iota$, and μ, i.e. by the classes ${}^1\iota$, ${}^1(Sq^2\iota)$, ${}^1\mu$. We next consider the path space over ${}^1\mathfrak{P}$ with fibre ${}^2\mathfrak{P}$ and compute in the same way. We note that ${}^2\mathfrak{P}$ has homotopy groups Z in dimensions 2 and 4 and all others trivial. Since $H^5(Z, 2; Z) = 0$, we must have ${}^2\mathfrak{P} = K(Z, 2) \times K(Z, 4)$. Thus the mod 2 cohomology of ${}^2\mathfrak{P}$ in dimensions up to 6 has as an additive basis $\{\alpha, \beta, \alpha^2, \alpha^3, \alpha\beta, Sq^2\beta\}$, where $\dim \alpha = 2$ and $\dim \beta = 4$. Then we must have $\tau(\alpha) = {}^1\iota$, $d_3(\beta) = {}^1\iota \otimes \alpha$, $\tau(\alpha^2) = \tau(Sq^2\alpha) = Sq^2({}^1\iota)$, $d_3(\alpha^3) = {}^1\iota \otimes \alpha^2$, $d_3(\alpha\beta) = {}^1\iota \otimes \beta + \alpha \otimes {}^1\iota \otimes \alpha = {}^1\iota \otimes \beta + {}^1\iota \otimes \alpha^2$, and hence $\tau(Sq^2\beta) = {}^1\mu$. This means ${}^2\mu = Sq^2\beta$. But in the cohomology operation corresponding to ${}^2\mu$, we must factor out the image of Sq^2. Hence this operation is zero.

10. The operation Ψ_n. ([13])[6]

Let $\mathfrak{P}_n = \mathfrak{P}(Z, 2; Z, 2n+1, C^{n+1})$, where C^{n+1} is the $(n+1)$-st power of the basic class $C \in H^2(Z, 2; Z)$. Let $p \colon \mathfrak{P}_n \to K(Z, 2)$ be the fibre map, and let $\iota \in H^2(Z, 2; Z_2)$ and $\iota' \in H^{2n+1}(Z, 2n+1; Z_2)$ be generators. Then $d_{2n+1}(\iota') = \tau(\iota') = \iota^{n+1}$ so that $d_{2n+1}(\iota \otimes \iota') = \iota^{n+2}$, and

$$d_{2n+3}(Sq^2\iota') = \tau(Sq^2\iota') = Sq^2\tau(\iota') = Sq^2(\iota^{n+1}) = \begin{cases} 0, & n\text{: odd} \\ \iota^{n+2} & n\text{: even.} \end{cases}$$

Since ι^{n+2} is in the image of d_{2n+1}, we have in any case

$$\tau(Sq^2\iota') = 0 \in E_{2n+4}{}^{2n+4,0}.$$

[6] Much of the material of this section is taken from [13].

It follows that $H^{2n+3}(\mathfrak{P}_n; Z_2) \approx Z_2$ and a generator ψ_n of this group has the property that $i^*(\psi_n) = Sq^2\iota' \in H^{2n+3}(Z, 2n+1; Z_2)$. Let Ψ_n be the secondary cohomology operation associated with ψ_n. Then Ψ_n is defined for any space X on those elements $h \in H^2(X)$ such that $h^{n+1} = 0 \in H^{2n+2}(X)$, and according to Theorem 3.6,

$$\Psi_n(h) \in H^{2n+3}(X; Z_2)/[Sq^2 + h \cup] H^{2n+1}(X; Z),$$

where the coefficient pairing $Z \otimes Z \to Z_2$ which defines the cup product is the Whitehead product pairing $\pi_{2n+1}(\mathfrak{P}_n') \otimes \pi_2(\mathfrak{P}_n') \to \pi_{2n+2}(\mathfrak{P}_n')$ in

$$\mathfrak{P}_n' = \mathfrak{P}_n(Z, 2; Z, 2n+1, C^{n+1}; Z_2, 2n+2, \psi_n).$$

LEMMA 10.1. *Let $P_n(C)$ denote complex-projective space of n complex dimensions. Then ψ_n is the second Postnikov invariant $k^{2n+3}(P_n(C))$ of $P_n(C)$.*

Proof. Obvious.

It follows from Lemma 10.1 that the Whitehead product

$$\pi_{2n+1}(\mathfrak{P}_n') \otimes \pi_2(\mathfrak{P}_n') \to \pi_{2n+2}(\mathfrak{P}_n')$$

is the same as the Whitehead product

$$\pi_{2n+1}(P_n(C)) \otimes \pi_2(P_n(C)) \to \pi_{2n+2}(P_n(C)).$$

This product has been computed (see [13] or [17]) and is trivial for n odd and non-trivial for n even. Thus when n is odd, we see that the cup-product term in the denominator for Ψ_n vanishes, and we have

$$\Psi_n(h) \in H^{2n+3}(X; Z_2)/Sq^2 H^{2n+1}(X; Z), \qquad n\colon \text{odd},$$

while for n even, the cup-product is relative to the non-trivial coefficient pairing $Z \otimes Z \to Z_2$.

The next theorem illustrates one of the ways our main theorems can be used to find relations between primary and secondary cohomology operations, i.e., the computation of primary operations in the cohomology of spaces with two homotopy groups.

THEOREM 10.2. *Let X be a space, let n be odd, and let $h \in H^2(X)$ be such that $h^{n+1} = 0$. Then*

$$Sq^2\Psi_n(h) = 0 \in H^{2n+5}(X; Z_2).$$

Proof. Let $f\colon X \to K(Z, 2)$ be a map such that $f^*(\iota) = h$, where $\iota \in H^2(Z, 2; Z)$ is the basic class. Then according to Theorem 7.2,

$$\Psi_n(h) = Sq_f^2(h^{n+1})$$
$$\in H^{2n+3}(X;Z_2)/(f^*H^{2n+3}(Z,2;Z_2) + Sq^2H^{2n+1}(X;Z))$$
$$= H^{2n+3}(X;Z_2)/Sq^2H^{2n+1}(X;Z)$$

since the coefficient pairing in the cup-product term in Theorem 7.2 is trivial. Now

$$Sq^2\Psi_n(h) \in H^{2n+5}(X;Z_2)/Sq^2Sq^2H^{2n+1}(X;Z)$$
$$= H^{2n+5}(X;Z_2)/Sq^3Sq^1H^{2n+1}(X;Z) = H^{2n+5}(X;Z_2).$$

Furthermore, according to Theorem 7.1, (Φ_{2n+2} is the Adem operation of § 9) $Sq^2\Psi_n(h) = Sq^2Sq^2_f(h^{n+1}) = f^*\Phi_{2n+2}(\iota^{n+1})$ in

$$H^{2n+5}(X;Z_2)/(f^*Sq^2H^{2n+3}(Z,2;Z_2) + Sq^2f^*H^{2n+3}(Z,2;Z_2) + Sq^2Sq^2H^{2n+1}(X;Z))$$
$$= H^{2n+5}(X;Z_2).$$

But $\Phi_{2n+2}(\iota^{n+1}) \in H^{2n+5}(Z,2;Z_2)/Sq^2H^{2n+3}(Z,2;Z_2) = 0$, which proves the theorem.

11. Cohomology operations in fibre spaces. In this section we show how Theorem 6.1 can be applied to the problem of computing primary cohomology operations in the total space of a fibre space when one knows the cohomology structure of the fibre and the base. We restrict ourselves to the stable range for simplicity; we will obtain information which is not contained in the spectral sequence of a fibre space.

Let $p: E \to B$ be a fibre space with fibre F. Let $i: F \to E$ be the inclusion. As in Section 3, let $\theta \in H^{n'+1}(\pi, n; \pi')$, $\phi \in H^q(\mathfrak{P}; G)$ and let $\theta'(\iota') = i^*(\phi) \in H^q(\pi', n'; G)$. Let $h \in H^n(B;\pi)$ be such that $\theta(h) = 0$ and $\tau(v) = h$, where $v \in H^{n-1}(F;\pi)$. Note that $\tau({}^1\theta(v)) = \theta(\tau(v)) = \theta(h) = 0$. We assume that $n' \leqq$ the sum of the connectives of B and F and that $q < n + n'$.

THEOREM 11.1. *Let $x \in H^{n'}(E;\pi')$ be such that $i^*(x) = {}^1\theta(v)$. Then*

$$\theta'(x) = p^*\Phi(h) \in H^q(E;G)/\theta'p^*(H^{n'}(B;\pi')).$$

Proof. It follows immediately from Lemma 6.2 that

$$\theta_p(h) = x \in H^{n'}(E;\pi')/p^*(H^{n'}(B;\pi')) + {}^1\theta(H^{n-1}(E;\pi)).$$

Our theorem now follows from Theorem 6.1.

Remark. In the spectral sequence of the fibre space $p: E \to B$, $\theta'(x)$

$= 0 \in E_2{}^{0,q}$ and hence also is zero in $E_\infty{}^{0,q}$. Under our dimensional restrictions, this implies that $\theta'(x) \in \operatorname{Im} p^*$. Theorem 11.1 gives more precise information.

12. Cup products in fibre spaces. This section is the analog of Section 11 for cup products. Using Theorem 8.1, we show that certain cup products in the total space of a fibre space are images of Massey triple products in the base space. These results were known to Hirsch [4] and Massey [6] in the case of sphere bundles.

Let $p\colon E \to B$ be a fibre space. Let $u \in H^p(B)$, $v \in H^q(B)$, $w \in H^r(B)$, and let $\tau(x) = u$, where $x \in H^{p-1}(F)$. We assume that $u \cup v = 0$; hence the element $v \otimes x \in E_2{}^{q,p-1} \approx H^q(B; H^{p-1}(F))$ goes into 0 under each d_r and gives an element $\{v \otimes x\} \in E_\infty{}^{q,p-1}$. We assume further that $v \cup w = 0$ and hence that $(v \otimes x) \cup w = 0 \in E_2{}^{q+r,p-1}$.

THEOREM 12.1. *There exists an element $y \in H^{p+q-1}(E)$ which projects into $\{v \otimes x\} \in E_\infty{}^{q,p-1}$ and such that*

$$(-1)^{q+1} y \cup p^*(w) = p^*\langle u, v, w\rangle \in H^{p+q+r-1}(E)/p^*(H^{q+r-1}(B) \cup w).$$

Proof. In order to apply Theorem 8.1, we must show that a representative of $(-1)^{q+1} u \underset{p}{\overset{L}{\cup}} v$ projects onto $\{v \otimes x\} \in E_\infty{}^{q,p-1}$. Let $\bar{x} \in C^{p-1}(F) = E_0{}^{0,p-1}$ represent x. Then $\delta\bar{x} = p^\#(\bar{u}) \in C^p(E)$ for some representative $\bar{u}$ of u. $\bar{v} \cup \bar{x} \in E_0{}^{q,p-1}$ represents $v \otimes x \in E_2{}^{q,p-1}$, and $\delta(\bar{v} \cup \bar{x}) = (-1)^q \bar{v} \cup p^\#(\bar{u})$. $u \underset{p}{\overset{L}{\cup}} v$ has as representative $(-1)^{q+1}\bar{v} \cup \bar{x} + (-1)^q p^\#(a)$, where $\delta a = \bar{u} \cup \bar{v}$. Thus in $E_0{}^{q,p-1}$, $\bar{v} \cup \bar{x}$ is a representative of $(-1)^{q+1} u \underset{p}{\overset{L}{\cup}} v$, and the theorem is proved.

Remark. In case F is $(p-2)$-connected, then y is defined modulo $p^*(H^{p+q-1}(B))$ and the theorem gives a sharper result.

PRINCETON UNIVERSITY AND YALE UNIVERSITY.

REFERENCES.

[1] J. Adem, "The iteration of the Steenrod squares in algebraic topology," *Proceedings of the National Academy of Sciences*, vol. 38 (1952), pp. 720-726.

[2] H. Cartan and J. P. Serre, "Espaces fibrés et groupes d'homotopie, II. Applications," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, Paris, vol. 234 (1952), pp. 393-395.

[3] S. Eilenberg and S. MacLane, "On the groups $H(\pi, n)$, I," *Annals of Mathematics*, vol. 58 (1953), pp. 55-106.

[4] G. Hirsch, "L'Anneau de cohomologie d'un espace fibré en sphères," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, Paris, vol. 241 (1955), pp. 1021-1023.

[5] I. M. James, "Note on cup-products," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 374-383.

[6] W. S. Massey, "On the cohomology ring of a sphere bundle," *Journal of Mathematics and Mechanics*, vol. 7 (1958), pp. 265-289.

[7] F. P. Peterson, "Functional cohomology operations," *Transactions of the American Mathematical Society*, vol. 86 (1957), pp. 197-211.

[8] ——— and N. Stein, "Two formulas concerning secondary operations," *Reports—Seminar in topology*, University of Chicago, 1957.

[9] ——— and E. Thomas, "A note on non-stable cohomology operations," *Boletin de la Sociedad Matemática in Mexicana*, segunda serie, vol. 3 (1958), pp. 13-18.

[10] M. M. Postnikov, "Investigations in the homotopy theory of continuous mappings." *American Mathematical Society Translations*, Ser. 2, Vol. 7, pp. 1-134.

[11] J. P. Serre, "Cohomologie modulo 2 des complexes d'Eilenberg-MacLane," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 198-232.

[12] N. Shimada, "Homotopy classification of mappings of a 4-dimensional complex into a 2-dimensional sphere," *Nagoya Mathematical Journal*, vol. 5 (1953), pp. 127-144.

[13] N. Stein, *The third obstruction in complex projective spaces*, Thesis, Cornell University, 1957.

[14] H. Toda, "Generalized Whitehead products and homotopy groups of spheres," *Journal of the Institue of Polytechnics, Osaka City University*, vol. 3, Ser. A, pp. 43-82.

[15] H. Uehara and W. S. Massey, "The Jacobi identity for Whitehead products," *Algebraic geometry and topology*, Princeton, 1957.

[16] P. Olum, "Obstructions to extensions and homotopies," *Annals of Mathematics*, vol. 52 (1950), pp. 1-50.

[17] M. G. Barratt, I. M. James and N. Stein, "Whitehead products and projective spaces" (to appear).

[18] J. P. Meyer, "Whitehead products and Postnikov systems" (to appear).

COMPACTNESS OF CERTAIN MAPPINGS.*[1]

By G. T. WHYBURN.

1. Introduction. A mapping of one topological space onto another is *compact* provided the inverse image of each compact set in the range space is itself a compact set. When this property is present the action of the mapping is in most essential respects similar to that of a mapping on a compact domain space. In this paper our objective will be the development of conditions, in situations of interest, which will imply compactness of the mapping or properties closely related thereto and also to study the implications of these related properties.

Our spaces X and Y are always understood to be separable and metric. Other properties will be explicitly stated when they are assumed. The use of the word *mapping* in connection with a transformation $f(X) = Y$ always implies that the transformation is single valued and continuous.

2. Traces of mappings. If $f(X) = Y$ is a mapping and Y' is any subset of Y, a set X' in X which maps onto Y' under f, i. e., so that $f(X') = Y'$, is called a *trace* of Y'. We shall be concerned primarily with conditions under which certain sets have compact traces. We note that *any set in Y having a compact trace is automatically compact.* Also, a simple application of the Borel Theorem yields at once

(2.1) *If X and Y are locally compact, every compact set in Y has a compact trace if and only if each point of Y is interior to some set in Y having a compact trace or, equivalently, if each $y \in Y$ is interior to the image of some compact set in X.*

The set Y_0 of all points $y \in Y$ such that y is interior to the image of some compact set in S is open. Thus if we say that f has the *compact trace property* at such a point y, we have

* Received June 3, 1958.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under contract No. AF 49(638)-71 at the University of Virginia.

(2.2) *If X and Y are locally compact, the set Y_0 of all points in Y where f has the compact trace property is non-empty and open and its complement $F_0 = Y - Y_0$ is closed and non-dense.*

That F_0 is non-dense and hence Y_0 is non-empty follows by a simple category-type argument.[5] For if X is represented as the union $X = \sum_1^\infty K_n$ of compact sets with $K_{n+1} \supset K_n$, then for any open set U in Y, $f(K_m) \cdot U$ must contain an open set U_0 for some m by local compactness of Y; and $U_0 \subset Y_0$ by definition of Y_0.

It results automatically that the sets $X_0 = f^{-1}(Y_0)$ and $E_0 = f^{-1}(F_0)$ are open and closed respectively and that X_0 is non-empty. If F_0 is empty, so that f has the compact trace property at each if its points, we say that it *has the compact trace property.* Equivalently, in case of locally compact X and Y, f has this property provided every compact set in Y has a compact trace. We then have

(2.3) *If X and Y are locally compact, $f \mid X_0$ is a mapping of X_0 onto Y_0 having the compact trace property.*

A property very close to the compact trace property has been used recently by P. McDougle [1] in characterizing the invariance of metrizability under certain mappings. This property (called P_2) requires that for each $y \in Y$ there exist a compact subset C_y of $f^{-1}(y)$ such that y is interior to the image of every open set in X containing C_y. Indeed for X and Y locally compact, this is equivalent to the compact trace property as we now show.

(2.4) THEOREM. *If X and Y are locally compact, a mapping $f(X) = Y$ has property P_2 if and only if every compact set in Y has a compact trace.*

Proof. Property P_2 implies that every compact set K in Y has a compact trace. For if $y \in K$, by P_2 there exists a compact subset H_y of $f^{-1}(y)$ such that if U_y is an open set containing H_y, then y is interior to $f(U_y)$. For each $y \in K$ let use choose such a U_y so that $\bar{U}_y$ is compact. Then since K is interior to $\sum f(U_y)$, there exists a finite set of points $y_1, y_2, \cdots, y_n$ in Y such that K is interior to $\sum_1^n f(U_{y_i})$. Accordingly if H denotes the compact set

$$H = f^{-1}(K) \cdot \sum_1^n \bar{U}_i,$$

$f(H) = K$ so that H is a compact trace for K.

To prove the reverse implication, let $y \in Y$ and let V be a neighborhood of y in Y with $\bar{V}$ compact. Then if A is a compact trace of $\bar{V}$ and U is any open set containing $A \cdot f^{-1}(y)$, y must be interior to $f(U)$ because $f(A) = \bar{V}$ and $f \mid A$ is a compact mapping.

We recall that a mapping $f(X) = Y$ is *quasi-open* provided that each $y \in Y$ is interior to the image $f(U)$ of every open set U in X which contains a compact component of $f^{-1}(y)$. If in addition there exists a compact component of $f^{-1}(y)$ for each $y \in Y$, we say that f is *effectively quasi-open.* Then either (2.1) or (2.4) yields at once

(2.5) *If X and Y are locally compact, every effectively quasi-open mapping $f(X) = Y$ has the compact trace property, i.e., every compact set in Y has a compact trace.*

Also a mapping $f(X) = Y$ is *monotone* provided $f^{-1}(y)$ is a continuum (compact and connected) for each $y \in Y$. For such mappings on locally compact spaces, having a compact trace is equivalent to having a compact inverse for a subset of Y. For we have in general

(2.6) THEOREM. *If X is locally compact and $f(X) = Y$ is monotone, any set in Y which has a compact trace has a compact inverse.*

For if the compact set H in Y has a compact trace K so that $f(K) = H$, $f^{-1}(H)$ must be compact. For if not we could choose a sequence of points $x_1, x_2, \cdots$ in $f^{-1}(H)$ so that $\sum x_n$ has no limit point but if $y_n = f(x_n)$, the points y_n are all distinct and the sequence (y_n) converges to a point $y \in H$. Then if U is a conditionally compact open set containing $K + f^{-1}(y)$ and C is the boundary of U, we must have $C \cdot f^{-1}(y_n) \neq 0$ for almost all n since for each n, $f^{-1}(y_n)$ is connected and intersects K and contains x_n. However, as C is compact, this gives $C \cdot \limsup f^{-1}(y_n) \neq 0$, contrary to the facts that lim-sup $f^{-1}(y_n) \subset f^{-1}(y)$ (by continuity of f) and $f^{-1}(y) \subset U$.

(2.61) COROLLARY. *If X is locally compact and $f(X) = Y$ is monotone, for any compact set K in X, $f^{-1}f(K)$ is compact. If K is a continuum, so also is $f^{-1}f(K)$.*

(2.62) COROLLARY. *A montone mapping on a locally compact space is compact if and only if it has the compact trace property.*

Note. That it is insufficient, in the theorem just proven, to have point inverses compact is shown by the mapping of the interval $0 \leqq x < 2$ onto the interval $0 \leqq y \leqq 1$ defined by $y = x$ for $0 \leqq x \leqq 1$, $y = 2 - x$ for $1 \leqq x < 2$.

Here point-inverses are either single points or point pairs and every compact set has a compact trace but of course the compact interval $0 \leqq y \leqq 1$ does not have a compact inverse.

3. Compact boundary traces. We next develop some conditions under which compactness of the mapping is a consequence of assumptions concerning the traces or inverses of certain boundary sets in the range space. A connected locally compact separable metric space is called a *generalized continuum.* We prove first

(3.1) LEMMA. *Let $f(X) = Y$ be a mapping, where X and Y are locally connected generalized continua. Let U be a conditionally compact open set in Y with boundary C such that $f^{-1}(C)$ is compact. If the number of non-conditionally compact components of $Y - C$ is finite and $\geqq$ the number of such components of $X - f^{-1}(C)$, then $f^{-1}(\bar{U})$ is compact.*

Proof. Let $R_1, R_2, \cdots, R_k$ be the non-conditionally compact components of $X - f^{-1}(C)$ and $S_1, S_2, \cdots, S_l$ the non-conditionally compact components of $Y - C$. By hypothesis $k \leqq l$. Now $H = X - \sum_1^k R_i$ must be compact. For if not, by local compactness of X and compactness of $f^{-1}(C)$, infinitely many distinct components of $X - f^{-1}(C)$, would intersect the boundary F of a conditionally compact neighborhood V of $f^{-1}(C)$ so that F would contain a point x of the limit superior of this sequence of components. This clearly is impossible by local connectedness of V at x. Hence H is compact.

However, we must have $f^{-1}(\bar{U}) \subset H$. For since $f(R_i)$ is connected, for each i, and lies in $Y - C$, each S_j must contain one of the sets $f(R_i)$ because $f(H)$ is compact. Since $l \geqq k$, we must have $f(R_i) \subset \sum S_j \subset Y - \bar{U}$ for each i so that $f^{-1}(\bar{U}) \subset H$.

(3.2) THEOREM. *Let $f(X) = Y$ be a mapping, where X and Y are locally connected generalized continua having the property that there is an integer $k \geqq 1$ such that the complement of each compact set in X or in Y has exactly k non-conditionally compact components. If for each $y \in Y$ there exist arbitrarily small neighborhoods of y whose boundaries have compact inverses under f, then f is compact.*

This is an easy consequence of the lemma. For if K is any compact set in Y, for each $y \in Y$ there exists a conditionally compact open set U_y about y with boundary C_y such that $f^{-1}(C_y)$ is compact. It results from the lemma that $f^{-1}(\bar{U}_y)$ is compact. Since by the Borel Theorem a finite union

of the sets U_y covers K, it follows that $f^{-1}(K)$ lies in a compact subset of X and hence is compact.

As shown in § 3, for monotone mappings the requirement of having a compact inverse for a set can be replaced by that of having a compact trace. Thus we get

(3.3) THEOREM. *With the same conditions on X and Y as in* (3.2), *if the mapping $f(X) = Y$ is monotone and if for each $y \in Y$ there exist arbitrarily small neighborhoods of y whose boundaries have compact traces, then f is compact.*

These two theorems have interesting consequences, particularly in the cases of mappings of a real line onto itself or of one Euclidean space onto another. In these cases the complement of *every* compact set has exactly *two* or exactly *one* non-conditionally compact component. Hence we have

(3.21) COROLLARY. *Any mapping which has compact point inverses of a line onto a line is compact.*

For in this case each point y of the line Y has arbitrarily small neighborhoods with boundaries of pairs of points.

(3.31) *Any monotone mapping of one Euclidean space onto another such that each point of the range space is contained in arbitrarily small open sets whose boundaries have compact traces is a compact mapping.*

It is clear that a similar statement could be made about monotone mappings from any locally connected generalized continuuum which is the union of an increasing sequence of compact sets with connected complements onto any other such space.

4. Mappings on Bouwer Property spaces. A space X has the *Brouwer Property* [2] provided every subset of X which is homeomorphic with an open subset of X is necessarily open in X. Now it is not true in general that when two spaces are homeomorphic, any 1-1 mapping of one onto the other is necessarily a homeomorphism. Indeed we have that

Example. There exists a 1-1 *mapping of a plane locally connected generalized continuum onto itself which is not a homeomorphism.*

Let the space X consist of the whole x-axis, the positive y-axis L and the union

$$\sum_{n=1}^{\infty} C_n + R_{-n},$$

where, for each $n > 0$, C_n is the circle of radius $\frac{1}{3}$ in the upper half plane tangent to the x-axis at the point $(n, 0)$ and R_{-n} is the vertical ray in the upper half plane originating at the point $(-n, 0)$. For each point $(x, y) \in X - L$ let us define

$$h(x, y) = (x + 1, y);$$

and let h be defined on L so as to map it (1-1) and continuously onto C_1 by sending $(0, 0)$ into $(1, 0)$ and wrapping L around C_1 clockwise, say. Clearly this mapping $h(X) = X$ meets all our requirements.

It may be noted, however, that the space X does not have the Brouwer Property. We show next that such a mapping is not possible on spaces which do have this property.

(4.1) THEOREM. *If X and Y are homeomorphic locally compact spaces having the Bouwer Property, any* 1-1 *mapping of X onto Y is a homeomorphism.*

The proof may be accomplished by showing that h is an open mapping. To this end, let U be any open set in X, let $y \in h(U)$ and let x be a point of $f^{-1}(y)$ lying in U. Next let us choose an open set V containing x such that $\bar{V}$ is compact and lies wholly in U. Then $h \mid \bar{V}$ is a homeomorphism. Accordingly, the set $h(V)$ is homeomorphic with the open subset V of X and hence also homeomorphic with some open subset of Y because X and Y are homeomorphic. Thus $h(V)$ is open in Y by the Brouwer Property. Hence y is interior to $h(U)$ and h is open since $h(V) \subset h(U)$.

(4.2) THEOREM. *Let $f(X) = Y$ be monotone, where Y is locally compact, has the Brouwer Property and is homeomorphic with the natural decomposition space of f. Then f is compact.*

The natural decomposition space of f is the space Y' whose elements are the point inverses $f^{-1}(y)$, $y \in Y$, topologized by defining a set of such elements as open provided the set union of these elements is open in Y. The mapping f has the representation

$$f(x) = h\phi(x),$$

where $\phi(X) = Y'$ is the natural mapping of this decomposition and $h(Y') = Y$ is 1-1 and continuous. By hypothesis Y' and Y are homeomorphic and have the Brouwer Property. Accordingly, by (4.1), h is a homeomorphism. Also, since f is monotone and X is locally compact, the natural decomposition of f is upper-semi continuous so that ϕ is closed. Since it

has compact point inverses, ϕ is therefore compact. Hence f is compact, being the resultant of the superposition of two compact mappings.

(4.21) COROLLARY. *Any monotone mappings of a Euclidean manifold M onto itself whose natural decomposition space is homeomorphic with M is necessarily compact.*

In particular, *any monotone mapping of a line onto a line is compact,* a fact which is also a special case of (3.21) above.

5. Monotone mappings on a plane. A deeper consequence of the theorem just proven, though not nearly so easily obtained, is

(5.1) THEOREM. *Any monotone mapping of a plane onto a plane is compact.*

Let $f(X) = Y$ be monotone, where X and Y are planes. Then if no point inverse $f^{-1}(y)$ separates the plane X, this conclusion follows at once from (4.2) together with the well known theorem of R. L. Moore [3] to the effect that the natural decomposition space of f is itself a topological plane and thus is homeomorphic with Y. Thus we have only to show that no point inverse under f can separate X.

To this end, let $N = f^{-1}(y)$, where y is any point whatever of Y. By (2.2) it follows that if A is a sufficiently large closed 2-cell on X enclosing N, $f(A)$ will contain an open 2-cell V in Y. By (2.61) the set $H = f^{-1}f(A)$ is a continuum. Let C be a circle enclosing H, let Q be the component of $X - f^{-1}f(C)$ containing H and let E be its boundary. Again by (2.61), $f^{-1}f(C)$ is a continuum so that E also is a continuum. Accordingly, if we decompose the continuum $Q + E$ into the set E and the individual points of Q and let $\phi(Q + E) = S$ be the natural mapping of this decomposition, then S is a topological sphere.

Next we let $e = \phi(E)$ and decompose S into the point e and the sets $\phi f^{-1}(y)$, for all $y \in R$, where $R = f(Q)$, and let $g(S) = K$ be the natural mapping of this decomposition. Since each of the sets $\phi f^{-1}(y)$ is a continuum, it follows [4] that K is a cactoid.

Now let us define

$$h(x) = f\phi^{-1}g^{-1}(x), \qquad x \in K - g(e).$$

Then h is a 1-1 mapping of $K - g(e)$ onto R. Further, h is compact. For if $M \subset R$ is compact, $f^{-1}(M)$ is a closed set lying in Q and thus is compact.

Thus $\phi f^{-1}(M)$ is compact as is also $g\phi f^{-1}(M)$, which is identical with $h^{-1}(M)$. Hence h must be a homeomorphism.

Since R contains V, K must contain at least one topological sphere W. Let q be a non-cut point of K on W, where $q = g(e)$ if $g(e) \in W$, and let $Z = W - q$. Then Z is an open 2-cell and thus so also is $h(Z)$. Accordingly, $h(Z)$ is open in the space Y. Whence Z must be open in K and hence is open and closed in the connected set $K - q$. This gives $Z = K - q$ so that $K = W$ and $q = g(e)$. Since K is then a topological sphere, no point inverse of f lying in Q separates X so that, in particular, N does not separate X and the proof is complete.

It may be noted that, once we have shown that $h(Z)$ is open in Y, the proof may be completed by applying (2.1) and (2.62) instead of referring back to the first paragraph of this proof. For we then have y interior to $h(Z) = f(Q) \subset f(Q + C)$, and $Q + C$ is compact.

Note 1. Combining the theorem just proven with Moore's theorem [3] we can assert the following: *Given a monotone mapping $f(X) = Y$, where X is a plane and Y is a topological space, then Y is a topological plane if and only if the mapping f is compact and has point inverses which do not separate X.*

Note 2. For non-compact monotone mappings on a plane a considerable variety of image spaces is possible. For example, the complex z plane may be mapped monotonically onto the unit circle $|w| = 1$ by the mapping $w = e^{im(z)}$, where $m(z) = 2\pi r/r + 1$, $r = |z|$.

The proof given for (5.1) suffices to give the same conclusion under a somewhat weakened hypothesis as follows

(5.2) THEOREM. *Any monotone mapping of a plane X onto a locally compact space Y which contains an open 2-cell and in which every open 2-cell is an open set, is necessarily compact.*

If the first paragraph of the proof of (5.1) is omitted and the proof concluded as indicated in the paragraph just preceeding *Note* 1, the reasoning establishes (5.2) without further alteration. Of course, it results by Moore's theorem that the space Y even here is necessarily a topological plane.

UNIVERSITY OF VIRGINIA.

CHARACTERISTIC CLASSES AND HOMOGENEOUS SPACES, II.*

By A. Borel and F. Hirzebruch.

Chapter VI. Applications to Todd Genera.[1]

20. Integration over the fibre in $(B_T, B_G, G/T, \rho(T,G))$.

Throughout § 20, the coefficients for cohomology are the real numbers and will not be mentioned explicitly.

20.1. Let G be a compact connected Lie group, T a maximal torus, $2m$ the dimension of G/T, $\mathcal{E}$ an invariant almost complex structure on G/T, and $a_1, \cdots, a_m$ the roots of $\mathcal{E}$ (see 12.3, 13.4). $\mathcal{E}$ defines an *orientation* of G/T, and hence also an identification of $H^{2m}(G/T)$ with $\boldsymbol{R}$, which will always be used in this §. In the fibering $\xi = (B_T, B_G, G/T, \rho(T,G))$ (see [2, § 20] for its definition), the integration over the fibre is a linear map of $H^*(B_T)$ in $H^*(B_G)$ or of $H^{**}(B_T)$ into $H^{**}(B_G)$ which lowers degrees by $2m$, (see § 8).

The order q of $W(G)$ is equal to the Euler number $E(G/T)$ of G/T and the latter is equal to the value of the m-th Chern class on the fundamental cycle. Therefore, considering the a_i's as elements of $H^2(B_T)$, we have by 10.8

$$(a_1 \cdots a_m)[G/T] = q = \text{order } W(G), \tag{1}$$

where the left side denotes the value of $a_1 \cdots a_m$ on an oriented fibre.

G/T is totally non-homologous to zero in ξ for real coefficients and q is also the dimension of $H^*(G/T)$, [2, § 26]. Therefore $\rho^*(T,G)$, which will be abbreviated by π^*, is injective, and we can choose homogeneous elements $h_1, \cdots, h_q \in H^*(B_T)$ with $h_q = a_1 \cdots a_m$, whose restrictions to a fibre form a basis of $H^*(G/T)$; an element $x \in H^*(B_T)$ can then be written in one and only one way in the form

$$x = \pi^*(b_1)h_1 + \cdots + \pi^*(b_q)h_q \qquad (b_i \in H^*(B_G)) \tag{2}$$

* Received June 19, 1958.

[1] Part I of this paper appeared earlier in this Journal, Vol. 80 (1958), pp. 458-538. We refer to it for the notation and a general introduction.

and we have by 8.4(1) and (1) above that

$$x^\natural = q \cdot b_q. \tag{3}$$

For any $w \in W(G)$, the elements $w(h_1), \cdots, w(h_{q-1})$, $\operatorname{sgn} w \cdot h_q$ (see 2.6 for $\operatorname{sgn} w$), when restricted to a fibre, also form a base of $H^*(G/T)$. Therefore, if we apply w to (2) and use 8.4(1) again, we see that

$$(w(x))^\natural = \operatorname{sgn} w \cdot x^\natural. \tag{4}$$

20.2. Lemma. *Let $x \in H^*(B_T)$ be such that $w(x) = \operatorname{sgn} w \cdot x$ for all $w \in W(G)$. Then*

$$q \cdot x = \pi^*(x^\natural) \cdot a_1 \cdot \cdots \cdot a_m.$$

We may consider $H^*(B_T)$ as the ring of polynomials with real coefficients on the universal covering V_T of T. Let S_i be the symmetry to the hyperplane $a_i = 0$. Then, $S_i(x) = -x$ implies that x is zero on $a_i = 0$, and hence that x is divisible by a_i. It follows that $x = y \cdot a_1 \cdots a_m$ with $y \in H^*(B_T)$ and, in view of our assumption, invariant under $W(G)$. Therefore [2, § 26], $y = \pi^*(b)$, $b \in H^*(B_G)$, and the lemma follows from (3).

20.3. Theorem. *Let $a_1, \cdots, a_m$ be the roots of an invariant almost complex structure $\mathcal{B}$ on G/T, and $\natural$ be the integration over the fibre in $(B_T, B_G, G/T, \pi)$ with respect to the orientation defined by $\mathcal{B}$. Then for $x \in H^*(B_T)$, we have*

$$\sum_{w \in W(G)} \operatorname{sgn} w \cdot w(x) = \pi^*(x^\natural) \cdot a_1 \cdot \cdots \cdot a_m. \tag{5}$$

Let y be the left-hand side of (5). Then $y^\natural = q \cdot x^\natural$ by (4). On the other hand, we have $w(y) = \operatorname{sgn} w \cdot y$ for any $w \in W(G)$; therefore 20.2 shows

$$q \cdot y = \pi^*(y^\natural) \cdot a_1 \cdot \cdots \cdot a_m$$

which proves the theorem.

It follows from 20.3 that, if $x \in H^{**}(B_T)$, then

$$\sum_{w \in W(G)} \operatorname{sgn} w \cdot w(x) = \pi^{**}(x^\natural) \cdot a_1 \cdots a_m. \tag{6}$$

21. Multiplicative sequences.

21.1. In this paragraph, ξ is a bundle in which F_ξ is a compact connected n-dimensional oriented manifold, G_ξ is a group of diffeomorphisms of F_ξ, and $\hat{\xi}$ is the bundle along the fibres (7.4). Γ is a commutative ring with unit and the cohomology groups of the fibres of ξ with respect to Γ are

assumed to form a constant sheaf on B_ξ. Then $\natural = \natural_\xi$ is a map of $H^{**}(E_\xi, \Gamma)$ into $H^{**}(B_\xi, \Gamma)$ which lowers degrees by n. In particular, we have

$$a^\natural = a[F_\xi] \cdot 1 \qquad (a \in H^n(E_\xi, \Gamma)), \tag{1}$$

where 1 is the unit of $H^{**}(B_\xi, \Gamma)$.

21.2. Let $\{K_j(p_1, \cdots, p_j)\}$ be a multiplicative sequence of polynomials in indeterminates p_i, with coefficients in Γ [19, § 1]. If η is a real vector bundle, we put

$$\mathcal{K}_\eta = \sum_{j \geqq 0} K_j(p_1(\eta), \cdots, p_j(\eta)). \tag{2}$$

We have $K_j(p_1(\eta), \cdots, p_j(\eta)) \in H^{4j}(B_\eta, \Gamma)$ and $\mathcal{K}_\eta \in H^{**}(B_\eta, \Gamma)$. If η is the tangent bundle to a compact oriented differentiable manifold X, then the genus $K(X)$ of X with respect to the sequence $\{K_j\}$ is defined by $K(X) = \mathcal{K}_\eta[X]$, i.e.

$$K(X) = K_r(p_1(\eta), \cdots, p_r(\eta))[X] \in \Gamma$$

if $4r = \dim X$, and $K(X) = 0$ if $\dim X \not\equiv 0 \bmod 4$.

21.3. Definition. *Let $\hat{\xi}$ be the bundle along the fibres of ξ. The multiplicative sequence $\{K_j\}$ is said to be strictly multiplicative in ξ if and only if*

$$(\mathcal{K}_{\hat{\xi}})^\natural \in H^0(B_\xi, \Gamma). \tag{i}$$

Let $\hat{p}_i$ be the Pontrjagin classes of $\hat{\xi}$. The condition (i) is equivalent to

$$K_j(\hat{p}_1, \cdots, \hat{p}_j)^\natural = 0 \qquad (4j > n). \tag{ii}$$

The restriction of $\hat{\xi}$ to a fibre of ξ is the tangent bundle to the fibre. Therefore we have by (1) for any multiplicative sequence

$$(K_j(\hat{p}_1, \cdots, \hat{p}_j))^\natural = K(F_\xi) \cdot 1 \qquad (4j = \dim F_\xi), \tag{3}$$

and therefore $\{K_j\}$ is strictly multiplicative in ξ if and only if

$$(\mathcal{K}_{\hat{\xi}})^\natural = K(F_\xi) \cdot 1. \tag{4}$$

A multiplicative sequence is always strictly multiplicative in the product bundle, because in this case, $\hat{\xi}$ may be identified with the bundle induced from the tangent bundle to F_ξ by the projection of $E_\xi = B_\xi \times F_\xi$ onto F_ξ, and then (ii) is obviously true.

21.4. In addition to 21.1, we assume that ξ is a differentiable bundle (7.4), and that B_ξ, E_ξ are compact connected oriented manifolds, the

orientation of E_ξ being induced by those of B_ξ, F_ξ taken in this order. It follows then from the definition of the integration over the fibre (8.1) or from its equivalence with the Gysin homomorphism (8.3, remark) that

$$a[E_\xi] = a^\natural[B_\xi] \qquad (a \in H^*(E_\xi, \Gamma)).$$

Let η and η' be the tangent bundles to E_ξ and B_ξ respectively. We have an exact sequence (7.6):

$$0 \to \hat{\xi} \to \eta \to \pi^*\eta' \to 0, \qquad (\pi = \pi_\xi), \tag{5}$$

and the multiplication theorem (9.7) implies

$$p(\eta) = p(\hat{\xi}) \cdot \pi^* p(\eta') \qquad \bmod \operatorname{Tors} H^*(E_\xi, \boldsymbol{Z}),$$

where $\operatorname{Tors} H^*(E_\xi, \boldsymbol{Z})$ is the torsion subgroup of $H^*(E_\xi, \boldsymbol{Z})$. By the fundamental property of multiplicative sequences [19, § 1.2], this yields

$$\mathcal{K}_\eta = \mathcal{K}_{\hat{\xi}} \cdot \mathcal{K}_{\pi^*\eta'} = \mathcal{K}_{\hat{\xi}} \cdot \pi^*(\mathcal{K}_{\eta'}), \tag{6}$$

modulo the image of $\operatorname{Tors} H^*(E_\xi, \boldsymbol{Z}) \otimes \Gamma$ in $H^*(E_\xi, \Gamma)$.

If $E_\xi = B_\xi \times F_\xi$, then [19, § 5.2]

$$K(E_\xi) = K(B_\xi) \cdot K(F_\xi). \tag{7}$$

More generally, we have

21.5. Proposition. *Let ξ be a differentiable bundle satisfying the assumption* 21.4 *and let $\{K_j\}$ be a multiplicative sequence of polynomials with coefficients in Γ. If $\{K_j\}$ is strictly multiplicative in ξ, then $K(E_\xi) = K(B_\xi) \cdot K(F_\xi)$.*

Since $H^j(E_\xi, \boldsymbol{Z})$ has no torsion for $j = \dim E_\xi$, we get from 21.4 and 8.2

$$K(E_\xi) = \mathcal{K}_\eta[E_\xi] = (\mathcal{K}_{\hat{\xi}} \cdot \pi^*\mathcal{K}_{\eta'})^\natural[B_\xi] = \mathcal{K}_{\eta'}(\mathcal{K}_{\hat{\xi}})^\natural[B_\xi],$$

and 21.5 follows from 21.2, 21.3(4).

21.6. We repeat briefly this discussion for the case of Chern classes. Let $\{K_j(c_1, \cdots, c_j)\}$ be a multiplicative sequence of polynomials with coefficients in Γ, in indeterminates c_i. Given a complex vector bundle η, we introduce the elements $K_j(c_1(\eta), \cdots, c_j(\eta)) \in H^{2j}(X, \Gamma)$ and put

$$\mathcal{K}_\eta = \sum_{j \geqq 0} K_j(c_1(\eta), \cdots, c_j(\eta)).$$

It is an element of $H^{**}(X, \Gamma)$. If η is the complex tangent bundle to a compact connected almost complex manifold (7.3), canonically oriented, the

genus of X with respect to $\{K_j\}$ or its "K-genus" is $K(X) = \mathcal{K}_\eta[X]$. It is equal to $K_m(c_1(\eta), \cdots, c_m(\eta))[X]$ if m is the complex dimension of X.

21.7. Let ξ be as in 21.1. Assume moreover that $\hat{\xi}$ has been endowed with a complex structure $\hat{\xi}_C$ of the type considered in 7.4, that is, defined by means of an almost complex structure of F_ξ, invariant under G_ξ, and let $\hat{c}_i$ be its Chern classes. The multiplicative sequence $\{K_j\}$ is then said to be strictly multiplicative in ξ with respect to $\hat{\xi}_C$ if one of the three following equivalent conditions is fulfilled

(i) $$(\mathcal{K}_{\hat{\xi}_C})^\natural \in H^0(B_\xi, \Gamma)$$

(ii) $$(K_j(\hat{c}_1, \cdots, \hat{c}_j))^\natural = 0, \qquad (2j > \dim F_\xi)$$

(iii) $$(\mathcal{K}_{\hat{\xi}_C})^\natural = K(F_\xi) \cdot 1.$$

21.8. Let ξ and $\hat{\xi}_C$ be as before. Assume in addition that ξ is differentiable and that B_ξ carries an almost complex structure η'_C. Then an almost complex structure η_C of E_ξ is said to be *compatible with* η'_C and $\hat{\xi}_C$ if there is an exact sequence

$$0 \to \hat{\xi}_C \to \eta_C \to \pi^*(\eta'_C) \to 0, \qquad (\pi = \pi_\xi). \tag{8}$$

Since exact sequences of vector bundles of the type (5), (8) always split, η_C always exists and is determined up to isomorphism by η'_C and $\hat{\xi}_C$. The proof of the following propostition is exactly the same as in the case of Pontrjagin classes:

21.9. PROPOSITION. *We keep the assumptions of* 21.8 *and assume moreover that the multiplicative sequence* $\{K_j\}$ *is strictly multiplicative in* ξ *with respect to* $\hat{\xi}_C$. *Then* $K(E_\xi) = K(B_\xi) \cdot K(F_\xi)$.

22. The Todd genus of certain almost complex homogeneous spaces. Throughout this paragraph, all cohomology groups will be taken with real coefficients, and all characteristic classes which occur will be regarded as real classes unless otherwise mentioned. The symbol $\boldsymbol{R}$ will be omitted in real cohomology groups.

22.1. *Notation.* Let ξ and η be complex vector bundles with the same base space: $B = B_\xi = B_\eta$. We recall that the Todd multiplicative sequence $\{T_j(c_1, \cdots, c_j)\}$ has $x(1 - e^{-x})^{-1}$ as its characteristic power series [19, § 1] and define the cohomology class $\mathcal{T}(\xi, \eta) \in H^{**}(B)$ by the equation

$$\mathcal{T}(\xi, \eta) = \mathrm{ch}(\eta) \sum_{j=0}^{\infty} T_j(c_1(\xi), \cdots, c_j(\xi)),$$

where $c_i(\xi) \in H^{2i}(B)$ is the i-th Chern class of ξ and $\mathrm{ch}(\eta)$ is the Chern character of η as defined in 9.1. For $d \in H^2(B)$, set

$$\mathcal{T}(\xi, d) = e^d \cdot \sum_{j=0}^{\infty} T_j(c_1(\xi), \cdots, c_j(\xi))$$

and for $d = 0$,

$$\mathcal{T}(\xi, 0) = \mathcal{T}(\xi).$$

It is clear that $\mathcal{T}(\xi, d) = \mathcal{T}(\xi, \eta)$ if η is the complex line bundle with d as its first Chern class.

More generally, as in [19, § 1], let $\{T_j(y; c_1, \cdots, c_j)\}$ be the generalized Todd sequence. This multiplicative sequence has

$$x(1+y)/(1-e^{-x(1+y)}) - yx$$

as its characteristic power series. We define $\mathcal{T}_y(\xi) \in H^{**}(B) \otimes \mathbf{R}[y]$ by the equation

$$\mathcal{T}_y(\xi) = \sum_{j=0}^{\infty} T_j(y; c_1(\xi), \cdots, c_j(\xi)).$$

Obviously, $\mathcal{T}_0(\xi) = \mathcal{T}(\xi)$.

If B is a compact almost complex manifold and if now ξ stands for the tangential complex vector bundle of B, then we set

$$\mathcal{T}(B, \eta) = \mathcal{T}(\xi, \eta), \qquad \mathcal{T}(B, d) = \mathcal{T}(\xi, d), \qquad \mathcal{T}_y(B) = \mathcal{T}_y(\xi).$$

Moreover, in agreement with the notations of [19, §§ 10, 11, 12], the following real numbers (respectively polynomials with real coefficients) are defined

$$T(B, \eta) = \mathcal{T}(B, \eta)[B],$$

$$T(B, d) = \mathcal{T}(B, d)[B],$$

$$T_y(B) = \mathcal{T}_y(B)[B] = \sum_{p=0}^{n} T^p(B) y^p, \text{ where } n = \dim_{\mathbf{C}} B.$$

$T(B)$ denotes the Todd genus $(T(B) = T_0(B) = T(B, 0))$.

Finally, let us recall the following formal fact: If c_i is the i-th elementary symmetric function in $\gamma_1, \cdots, \gamma_n$ ($c_i = 0$ for $i > n$), then

$$\sum_{j=0}^{\infty} T_j(c_1, \cdots, c_j) = e^{c_1/2} \prod_{i=1}^{n} \gamma_i/(2 \sinh(\gamma_i/2)).$$

22.2. Let G be a compact connected Lie group and T a maximal torus of G. Let V be the universal covering of T and $a_1, \cdots, a_m$ the *positive* roots of G with respect to an ordering $\mathcal{S}$ on V^* (2.4). Let ξ be a principal G-bundle and ξ_C the complex vector bundle along the fibres (7.4) of

$(E_\xi/T, B_\xi, G/T, \pi)$ which belongs to the invariant almost complex structure on G/T having $\epsilon_1 a_1, \epsilon_2 a_2, \cdots, \epsilon_m a_m$, $(\epsilon_i = \pm 1)$, as its roots (12.3 and 13.4). We orient G/T according to this almost complex structure and denote by $\natural$ the integration over the fibre with respect to this orientation (8.1). The total Chern class of $\hat{\xi}_C$ is given by the formula (10.8):

$$(1) \qquad c(\hat{\xi}_C) = (1 + \epsilon_1 a_1)(1 + \epsilon_2 a_2) \cdots (1 + \epsilon_m a_m).$$

Now let d be an arbitrary element of $H^1(T) = V^*$. We may regard d as an element of $H^2(E_\xi/T)$ under the negative transgression. Then, using (1) for the cohomology class $\mathcal{T}(\hat{\xi}_C, d)$ introduced in 22.1, we have

$$\mathcal{T}(\hat{\xi}_C, d) = e^d \cdot \prod \epsilon_j a_j / (1 - \exp(-\epsilon_j a_j)) = e^{(c_1/2)+d} \prod_{j=1}^{m} a_j / (2 \sinh(a_j/2)),$$

where $c_1 = c_1(\xi_C) = \sum_{i=1}^{m} \epsilon_i a_i$. We are going to calculate $\mathcal{T}(\hat{\xi}_C, d)^\natural$ by 20.3. In view of 8.3, this is possible since ξ is induced from the universal bundle. First observe that $\prod a_j/(2\sinh(a_j/2))$ is invariant under the operations of the Weyl group $W(G)$ since the roots are permuted up to sign and since $x/\sinh x$ is an even function in x. Thus we obtain, after setting $b = d + \frac{1}{2} c_1(\hat{\xi}_C)$ and $a = \sum_{j=1}^{m} a_j$,

$$\epsilon_1 \epsilon_2 \cdots \epsilon_m \pi^{**}(\mathcal{T}(\hat{\xi}_C, d)^\natural) = \sum_{w \in W(G)} \operatorname{Sgn}(w) e^{w(b)} / \prod_{i=1}^{m} 2 \sinh a_i/2$$

or, in the notations of 3.2:

$$(2) \qquad \epsilon_1 \epsilon_2 \cdots \epsilon_m \pi^{**}(\mathcal{T}(\hat{\xi}_C, d)^\natural) = E(b/2\pi(-1)^{\frac{1}{2}}) / E(a/4\pi(-1)^{\frac{1}{2}}).$$

It follows that $\mathcal{T}(\hat{\xi}_C, d)^\natural$ vanishes if b is singular. The right side of the preceding equation is a formal power series in $d, a_1, \cdots, a_m$ (regarded as elements of $H^2(E_\xi/T)$) and, as such, is an element of $H^{**}(E_\xi/T)$. On the other hand, $d, a_1, \cdots, a_m$ are originally elements of V^*, i.e. functions on V. If b is a non-singular weight, then $E(b)/E(a/2)$ is also a function on V, namely, up to a sign, the character of a certain irreducible representation of $\tilde{G}$ (for $\tilde{G}$, see 3.3). In fact, if b is a non-singular weight, then there is a unique element $w' \in W(G)$ such that $w'(b)$ is in the positive Weyl chamber (2.7) with respect to the ordering $\mathcal{S}$; i.e., $(w'(b), a_j) > 0$ for $1 \leqq j \leqq m$, and hence $w'(b) - a/2$ is the highest weight of an irreducible representation λ of $\tilde{G}$ which is uniquely determined up to equivalence. According to 3.4, the function $E(b)/E(a/2)$ on V equals the character of λ as a function on V multiplied by $\operatorname{Sgn}(w')$. Thus we have seen that $\mathcal{T}(\xi_C, d)^\natural$ is essentially given by a character.

It is clear that $w'(b) - a/2$ is integral on the unit lattice of G if and only if d has this property. Assume now that d has the property just mentioned (in other words, that $d \in H^1(T, \boldsymbol{Z}) \subset H^1(T) = V^*$) and that $b = d + \frac{1}{2}c_1(\hat{\xi}_C)$ is non-singular. Then λ also defines a representation of G. The λ extension (6.5) $\lambda(\xi)$ of the principal G-bundle ξ is then defined. It is a $\boldsymbol{U}(n)$-bundle and we have

$$\mathcal{T}(\hat{\xi}_C, d)^\natural = \operatorname{Sgn}(w')\epsilon_1\epsilon_2 \cdots \epsilon_m \cdot \operatorname{ch}(\lambda(\xi)). \tag{3}$$

Here ch is the Chern character as defined in 9.1. See also 10.2, 10.3.

22.3. In Sections 22.3 and 22.4, we shall apply the results of 22.2 to the very special case where B_ξ is a point; then $E_\xi = G$ and $E_\xi/T = G/T$. Every element of V^* may be regarded as an element of $H^2(G/T)$. Otherwise, we keep the notations of 22.2.

The homogeneous space G/T has 2^m invariant almost complex structures belonging to the 2^m possible choices of the signs $\epsilon_1, \epsilon_2, \cdots, \epsilon_m$. Now endow G/T with the invariant almost complex structure having the roots $\epsilon_1 a_1, \epsilon_2 a_2, \cdots, \epsilon_m a_m$. Then the first Chern class of G/T is

$$c_1 = c_1(G/T) = \epsilon_1 a_1 + \epsilon_2 a_2 + \cdots + \epsilon_m a_m.$$

Since $a/2$ is a weight, $c_1/2$ is also a weight, which implies by (10.1) that the integral first Chern class $c_1(G/T) \in H^2(G/T, \boldsymbol{Z})$ equals 0 when reduced to coefficients mod 2. *Thus the second Stiefel-Whitney class $w_2(G/T) \in H^2(G/T, \boldsymbol{Z}_2)$ vanishes.*

The Pontrjagin class p_i of G/T is the i-th elementary symmetric function in the a_j^2, and vanishes for $i > 0$ (10.9). Thus for $d \in H^2(G/T)$ (see end of 22.1),

$$\begin{aligned} &\mathcal{T}(G/T, d) = \exp(d + \tfrac{1}{2}c_1) \in H^*(G/T), \\ &m! \cdot T(G/T, d) = ((c_1/2) + d)^m[G/T], \\ &2^m m! \cdot T(G/T) = c_1{}^m[G/T]. \end{aligned} \tag{4}$$

On the other hand, in our special case, $T(G/T, d) \cdot 1 = \mathcal{T}(G/T, d)^\natural$ and we have, by 22.2, for an element $d \in V^*$, that

$$T(G/T, d) = 0 \text{ if } d + (c_1/2) \text{ is singular,} \tag{5}$$

$$T(G/T, d) = \pm \deg(\lambda), \tag{6}$$

if d is a non-singular weight, and if λ is a suitable representation.

By Theorem 4.3, the sum $c_1 = \epsilon_1 a_1 + \cdots + \epsilon_m a_m$ is non-singular if and

only if $\epsilon_1 a_1, \cdots, \epsilon_m a_m$ is a positive system of roots of G. By 4.9 and 12.4, we get that $\epsilon_1 a_1 + \cdots + \epsilon_m a_m$ is non-singular if and only if the invariant almost complex structure on G/T with roots $\epsilon_1 a_1, \cdots, \epsilon_m a_m$ is integrable.

Putting the value 0 for d in (5), we see that the Todd genus of G/T endowed with a non-integrable invariant almost complex structure vanishes. If, however, the structure is integrable, i.e., c_1 is non-singular, then (for $d=0$) we have in the notation of 22.2 that $w'(\frac{1}{2}c_1) = w'(b) = a/2$ and $\operatorname{Sgn}(w') = \epsilon_1\epsilon_2 \cdots \epsilon_m$. Thus λ is the trivial representation of degree 1 and the Todd genus of G/T equals $\deg(\lambda) = 1$.

22.4. Let $a_1, a_2, \cdots, a_m$ be as before the positive system of roots of G with respect to some ordering $\mathcal{S}$ and let $a = \sum_{j=1}^{m} a_j$. Choose the integrable invariant almost complex (i.e. complex) structure on G/T which has $a_1, a_2, \cdots, a_m$ as its roots ($\epsilon_i = 1$) and let G/T be oriented accordingly. An arbitrary element $b \in V^*$ can be regarded as element of $H^2(G/T)$ and then the number $\delta(b) = b^m[G/T]/m!$ is defined. δ defines a homogeneous polynomial of degree m on V^*, which vanishes if $(b, a_j) = 0$, see (4) and (5). Since a_i and a_j are not proportional for $i \neq j$ and since $\delta(a/2) = 1$ by (4), we get

$$(7) \qquad b^m[G/T] = m! \prod_{j=1}^{m} (b, a_j)/(a/2, a_j), \qquad (b \in V^*).$$

Formula (7) shows that b *is singular if and only if* $b^m[G/T] = 0$.

Theorem 20.3 implies immediately that

$$(8) \qquad b^m[G/T] = (a_1 a_2 \cdots a_m)^{-1} \sum_{w \in W(G)} \operatorname{Sgn}(w) w(b)^m,$$

where the right side of this equation has to be regarded as a quotient of two homogeneous polynomials of degree m on V. Assume now that b is a weight. Then b is in the positive Weyl chamber ($(b, a_j) > 0$ for $1 \leqq j \leqq m$) if and only if $b - a/2$ is in the closure of the positive Weyl chamber ($(b, a_j) \geqq 0$ for $1 \leqq j \leqq m$). By (3) and (6), we get:

If b is a weight contained in the positive Weyl chamber, then

$$(9) \qquad b^m[G/T]/m! = T(G/T, b - a/2) = \deg(\lambda),$$

where λ is the irreducible representation of $\bar{G}$ with main weight $b - a/2$, and a is the sum of the roots a_j of the invariant complex structure on G/T; i.e., a is the first Chern class of G/T endowed with this complex structure.

By (7) and (8), we get well known formulas for the degree of λ, see 3.4.

22.5. In this and the following Section, we shall use 22.2 to prove the strictly multiplicative behavior of the Todd sequence in certain fibre bundles. For this purpose, we take the value 0 for d in 22.2. Then $2b$ equals the first Chern class of the complex vector bundle $\hat{\xi}_C$ along the fibres of $(E_\xi/T, B_\xi, G/T, \pi)$. By 22.2 and 22.3, we see that the integration over the fibre (with respect to the orientation of G/T induced by $\hat{\xi}_C$) gives, when applied to $\mathcal{T}(\hat{\xi}_C)$, either 0 or $\mathrm{ch}(\lambda(\xi))$, where λ is the trivial 1-dimensional representation, and thus $\mathrm{ch}(\lambda(\xi))=1$. In either case, the integration over the fibre gives only a zero-dimensional term. According to the definition in 21.7, we get:

THEOREM. *Let ξ be a principle G-bundle. Choose an invariant almost complex structure on G/T and let $\hat{\xi}_C$ be the corresponding complex vector bundle along the fibres of $(E_\xi/T, B_\xi, G/T)$. Then the Todd sequence $\{T_j\}$ is strictly multiplicative in $(E_\xi/T, B_\xi, G/T)$ with respect to $\hat{\xi}_C$.*

For later use, we reformulate our result as follows: Let Ψ be a set of roots of G which contains for each root α exactly one of the roots α, $-\alpha$. Then Ψ is the set of roots of an invariant almost complex structure on G/T. Orient G/T by this structure and let $\natural(\Psi)$ be the integration over the fibre in $(E_\xi/T, B_\xi, G/T)$ with respect to that orientation. Then we have

$$(10)\qquad \Big(\prod_{\alpha\in\Psi}\alpha/(1-e^{-\alpha})\Big)^{\natural(\Psi)}=\begin{cases}1, & \text{if } \Psi \text{ is a positive system}\\ 0, & \text{otherwise.}\end{cases}$$

Let ϵ be a map of Ψ into $\{1,-1\}$ and $s(\epsilon)$ the number of elements in Ψ which are mapped by ϵ on -1, and let $\mathrm{sgn}(\epsilon)=(-1)^{s(\epsilon)}$. We have

$$\prod_{\alpha\in\Psi}\epsilon(\alpha)\cdot\alpha/(1-e^{-\epsilon(\alpha)\cdot\alpha})=\exp\Big(\tfrac{1}{2}\sum_{\alpha\in\Psi}\epsilon(\alpha)\cdot\alpha\Big)\cdot\prod_{\alpha\in\Psi}\alpha/(2\sinh(\alpha/2)).$$

Thus, by (10),

$$(10^*)\qquad \Big(\exp\Big(\tfrac{1}{2}\sum_{\alpha\in\Psi}\epsilon(\alpha)\cdot\alpha\Big)\cdot\prod_{\alpha\in\Psi}\alpha/(2\sinh(\alpha/2))\Big)^{\natural(\Psi)}$$

is equal to $\mathrm{sgn}(\epsilon)\cdot 1$, if $\{\epsilon(\alpha)\cdot\alpha \mid \alpha\in\Psi\}$ is a positive system, and to 0, otherwise.

We give two applications of formula (10): Let ξ be a principal G-bundle for which B_ξ is a compact *oriented* manifold. Let Ψ be a *positive* system of roots of G. Orient G/T accordingly and choose for E_ξ/T that orientation which is induced by those of B_ξ and G/T. Then, for $y\in H^*(E_\xi/T)$,

we have (see 21.4):

$$y[E_\xi/T] = y^{\natural(\Psi)}[B_\xi].$$

This fact, together with (10) and 8.2, yields for every element x of $H^*(B_\xi)$ that

$$x[B_\xi] = (\pi^*(x) \cdot \prod_{\alpha \in \Psi} \alpha/(1 - \exp(-\alpha)))[E_\xi/T], \tag{11}$$

where π is the projection of E_ξ/T on B_ξ.

22.6. Now let ξ be again an arbitrary principal G-bundle. For a closed connected subgroup U of G which contains a maximal torus T of G, consider the diagram

$$E_\xi/T \xrightarrow{\pi_\nu} E_\xi/U \xrightarrow{\pi_\mu} B_\xi. \tag{12}$$

Orient G/U. Let Θ be a system of positive roots of U. Orient U/T by the invariant complex structure having Θ as its set of roots and give G/T the orientation induced by those of G/U and U/T.

According to the above diagram, we have the fibre bundles

$$\mu = (E_\xi/U, B_\xi, G/U, \pi_\mu), \qquad \nu = (E_\xi/T, E_\xi/U, U/T, \pi_\nu),$$

$$\tilde{\xi} = (E_\xi/T, B_\xi, G/T, \pi_{\tilde{\xi}}), \qquad \eta = (G/T, G/U, U/T, \pi_\eta),$$

which satisfy the assumptions of 8.4. (The ξ of 8.4 corresponds to the $\tilde{\xi}$ here and the θ of 8.4 to η.) If we define the integrations over the fibres with respect to the orientations already chosen, then formula (2) of 8.4 holds. Thus we can infer from (10) and 8.2 the

PROPOSITION. *Let x be an arbitrary element of $H^{**}(E_\xi/U)$. Then in the foregoing notation*

$$x^{\natural\mu} = (\pi_\nu^{**}(x) \cdot \prod_{\alpha \in \Theta} \alpha/(1 - e^{-\alpha}))^{\natural\tilde{\xi}}.$$

22.7. Let U be a closed connected subgroup of G containing a maximal torus T of G and assume that G/U has been endowed with an invariant almost complex structure $\mathscr{J}$. Thus G/U is oriented. Let Ψ be the set of the roots of $\mathscr{J}$ and Θ a system of positive roots of U according to which we orient U/T. Then G/T is oriented. Let ξ be again a principal G-bundle for which we consider the diagram (12) and the four fibre bundles μ, ν, $\tilde{\xi}$, η. We wish to prove that the generalized Todd sequence (22.1) is strictly multiplicative (21.7) in μ with respect to the complex vector bundle $\hat{\mu}_C$ along the fibres arising from the given invariant almost complex structure on G/U. Let n

be the complex dimension of G/U, i.e., the number of roots in Ψ. First we observe that $\pi_\nu^{**}(\mathcal{T}_y(\hat{\mu}_C))$ is, in virtue of 10.8, equal to the element

$$(13) \qquad \prod_{\alpha\in\Psi}((1+y)\alpha/(1-e^{-(1+y)\alpha})-y\alpha)\in H^{**}(E_\xi/T)\otimes \mathbf{R}[y]$$

which goes over into

$$(13^*) \qquad \prod_{\alpha\in\Psi}(1+ye^{-\alpha})\alpha/(1-\exp(-\alpha))\in H^{**}(E_\xi/T)\otimes \mathbf{R}[y]$$

if one multiplies the component of complex dimension i in (13) by $(1+y)^{n-i}$. We have to prove that $\mathcal{T}_y(\hat{\mu}_C)^{\natural\mu}$ is a zero-dimensional element of $H^{**}(B_\xi)$. In view of the proposition in 22.6 and the passage from (13) to (13*), we must prove that the element

$$(\prod_{\alpha\in\Psi}(1+ye^{-\alpha})\cdot\prod_{\beta\in\Theta\cup\Psi}\beta/(1-\exp(-\beta)))^{\natural\xi}$$

which is equal to

$$(14) \qquad (\exp(\sum_{\beta\in\Theta\cup\Psi}\beta/2)\cdot\prod_{\alpha\in\Psi}(1+ye^{-\alpha})\cdot\prod_{\beta\in\Theta\cup\Psi}\beta/(2\sinh(\beta/2)))^{\natural\xi}$$

is zero-dimensional. But this is a consequence of (10*). The set $\Theta\cup\Psi$ plays here the role of Ψ in (10*). Thus the element given in (14) equals the unit of $H^{**}(B_\xi)$ multiplied by $T_y(G/U)$, (G/U has the given almost complex structure). Here we have to use that in passing from (13) to (13*), the component of complex dimension n is not changed. Using (10*), we can obtain the value of $T_y(G/U)$. In order to formulate the final result more easily, we introduce the following definition.

DEFINITION. *Let U be a closed subgroup of G containing a maximal torus T of G. Let Ψ be a set of complementary roots of G with respect to U which contains for each complementary root α exactly one of the roots α, $-\alpha$. Let Θ be a system of positive roots of U. Then $k^p(G/U,\Psi,\Theta)$ is defined as the number of those positive systems of roots of G which contain Θ and exactly $n-p$ roots of Ψ and thus p roots of $-\Psi$ $(0\leq 2p\leq 2n=\dim_{\mathbf{R}} G/U)$.*

Using this definition, we have, in virtue of (10*) and the fact that the element given in (14) equals $T_y(G/U)\cdot 1$, that

$$(15) \qquad T_y(G/U)=\sum_{p=0}^{n}T^p(G/U)y^p=\sum_{p=0}^{n}(-y)^p k^p(G/U,\Psi,\Theta).$$

We notice that $k^p(G/U,\Psi,\Theta)$ depends only on Ψ and not on the choice of the positive system Θ of U if Ψ is the set of roots of an invariant almost complex structure on G/U. The number $k^p(G/U,\Psi,\Theta)$ is also well defined if G/U does not admit an invariant almost complex structure.

Formula (15) states in particular that the Todd genus $T(G/U)$ equals $k^0(G/U,\Psi,\Theta)$. Thus $T(G/U)$ equals 1 if $\Psi\cup\Theta$ is a positive system of roots of G and is 0 otherwise. If the invariant almost complex structure on G/U with Ψ as the set of its roots is integrable, then $\Psi\cup\Theta$ is a positive system (13.7) and thus $T(G/U)=1$. If $T(G/U)=1$, then $\Psi\cup\Theta$ is a positive system, but $\Psi\cup-\Theta$ is also positive, since $-\Theta$ is a system of positive roots of U and $k^0(G/U,\Psi,-\Theta)=T(G/U)=1$. Therefore, $T(G/U)=1$ implies that $\Psi\cup\Theta$, $\Psi\cup-\Theta$ are positive and thus closed systems. $\Theta\cup-\Theta$ is closed, since it is the set of roots of a subgroup. Thus $T(G/U)=1$ implies that $\Psi\cup\Theta\cup-\Theta$ is closed and that the given invariant almost complex structure is integrable (12.4).

We express the results of this section in the following theorem.

22.8. THEOREM. *Let G be a compact Lie group and U a closed connected subgroup of maximal rank of G. The Todd genus of an invariant almost complex structure on G/U equals* 1 (*respectively* 0) *if the structure is integrable* (*respectively not integrable*). *With respect to a maximal torus T $(T\subset U\subset G)$, let Θ be a system of positive roots of U. Assume that G/U has been given an invariant almost complex structure $\mathfrak{J}$ and that Ψ is the set of roots of $\mathfrak{J}$. Then, letting n be the complex dimension of G/U and using the definition in* 22.7, *we have*

$$T_y(G/U)=\sum_{p=0}^{n}T^p(G/U)y^p=\sum_{p=0}^{n}(-y)^pk^p(G/U,\Psi,\Theta).$$

Let ξ be a principal G-bundle. The generalized Todd sequence

$$\{T_j(y;c_1,\cdots,c_j)\}$$

is strictly multiplicative in $(E_\xi/U,B_\xi,G/U)$ with respect to the complex vector bundle along the fibres $\hat{\xi}_C$ arising from $\mathfrak{J}$. In particular, if B_ξ is a compact almost complex differentiable manifold, if ξ is differentiable and if the differentiable manifold E_ξ/U has been endowed with an almost complex structure compatible (21.8) *with the almost complex structure of B_ξ and $\hat{\xi}_C$, then*

$$T_y(E_\xi/U)=T_y(B_\xi)\cdot T_y(G/U).$$

22.9. For $y=1$, the preceding theorem gives results on the index $\tau(G/U)$, see [19, §§ 8 and 10]. These results remain correct for an arbitrary G/U not necessarily almost complex:

Let G be a compact connected Lie group and U a closed connected subgroup of G of maximal rank. Let T be a maximal torus of U. Then,

with respect to T, let Ψ be a set of complementary roots containing for each complementary root α exactly one of the roots $\alpha, -\alpha$. Let ξ be a principal G-bundle. The element $\prod_{\alpha \in \Psi} \alpha/\operatorname{tgh} \alpha \in H^{**}(E_\xi/T)$ is symmetric in the α^2 ($\alpha \in \Psi$), and thus belongs to $\pi_\nu^{**}(H^{**}(E_\xi/U))$. According to 10.7,

$$\prod_{\alpha \in \Psi} \alpha/\operatorname{tgh} \alpha = \pi_\nu^{**}\left(\sum_{j=0}^{\infty} L_j(p'_1, p'_2, \cdots, p'_j)\right),$$

where the p'_i are the Pontrjagin classes of the real vector bundle $\hat{\mu}$ along the fibres of $(E_\xi/U, B_\xi, G/U)$. (For the L_j, see [19, § 1].) We orient the bundle along the fibres and thus also G/U by requiring that

$$\prod_{\alpha \in \Psi} \alpha = \pi_\nu^{**}(W_{2n}),$$

where W_{2n} denotes the Euler class of $\hat{\mu}$ ($2n = \dim_R G/U$). Then the same calculations as in 22.7 show that $\{L_j\}$ is strictly multiplicative in $(E_\xi/U, B_\xi, G/U)$ and that

$$\tau(G/U) = \sum_{p=0}^{n} (-1)^p k^p(G/U, \Psi, \Theta),$$

Θ being an arbitrary system of positive roots of U. As a consequence of the strictly multiplicative behavior, we have

$$\tau(E_\xi/U) = \tau(B_\xi) \cdot \tau(G/U),$$

in case B_ξ is a compact oriented differentiable manifold and ξ a differentiable bundle and after introducing convenient orientations.

In a similar way, under the assumptions of this section, we get by setting $y = -1$ for the Euler number $E(G/U)$ that

$$E(G/U) = \sum_{p=0}^{n} k^p(G/U, \Psi, \Theta).$$

22.10. The strictly multiplicative behavior (22.8) of the Todd sequence has certain formal consequences. We follow the notations of 22.7. Let ξ be a differentiable principal G-bundle over the compact almost complex differentiable manifold B_ξ and η a complex vector bundle over B_ξ. Consider the bundle $\mu = (E_\xi/U, B_\xi, G/U, \pi_\mu)$ and the complex vector bundle $\hat{\mu}_C$ along the fibres arising from a given invariant almost complex structure on G/U. Then endow E_ξ/U with an almost complex structure compatible with that of B_ξ and with $\hat{\mu}_C$. We have

$$\mathcal{T}(E_\xi/U, \pi_\mu^*\eta)^{\natural\mu} = T(G/U) \cdot \mathcal{T}(B_\xi, \eta). \tag{16}$$

Proof. Since the complex tangent bundle of E_ξ/U is the Whitney sum of $\hat{\mu}_C$ and the complex tangent bundle of B_ξ lifted under π_μ, we obtain from the Whitney multiplication theorem (9.7) that

$$\mathfrak{T}(E_\xi/U) = \mathfrak{T}(\hat{\mu}_C) \cdot \pi_\mu{}^* \mathfrak{T}(B_\xi).$$

Thus

$$\begin{aligned}\mathfrak{T}(E_\xi/U, \pi^*{}_\mu \eta)^{\natural\mu} &= (\pi_\mu{}^*(\operatorname{ch}(\eta)) \cdot \pi_\mu{}^*(\mathfrak{T}(B_\xi)) \cdot \mathfrak{T}(\hat{\mu}_C))^{\natural\mu} \\ &= \mathfrak{T}(\hat{\mu}_C)^{\natural\mu} \cdot \mathfrak{T}(B_\xi, \eta) = T(G/U) \cdot \mathfrak{T}(B_\xi, \eta),\end{aligned}$$

which completes the proof.

As a consequence of (16), we get (see 21.4):

$$T(E_\xi/U, \pi_\mu{}^*\eta) = T(G/U) \cdot T(B_\xi, \eta). \tag{17}$$

There is a formula for the generalized Todd sequence which is analogous to (16) and which follows from the strictly multiplicative behavior of the generalized Todd sequence. In order to write it down, we introduce the element $\operatorname{ch}_y(\eta)$ as the element obtained from $\operatorname{ch}(\eta)$ by multiplying its component of complex dimension j with $(1+y)^j$. The element $\operatorname{ch}_y(\eta)$ was denoted by $\mathrm{t}_y(\eta)$ in [19, § 12.2]. We have

$$(\operatorname{ch}_y(\pi_\mu{}^*\eta) \cdot \mathfrak{T}_y(E_\xi/U))^{\natural\mu} = T_y(G/U) \cdot \operatorname{ch}_y(\eta) \mathfrak{T}_y(B_\xi), \tag{18}$$

which implies

$$T_y(E_\xi/U, \pi_\mu{}^*\eta) = T_y(G/U) \cdot T_y(B_\xi, \eta). \tag{19}$$

For the definition of $T_y(B_\xi, \eta)$ and $T_y(E_\xi/U, \pi_\mu{}^*\eta)$, see [19, § 12]. Compare also [19, § 14.4].

22.11. Let G be a compact connected Lie group, U a closed connected subgroup of maximal rank and T a maximal torus of U. Let d be an element of $H^1(T, \boldsymbol{Z})$ which is orthogonal to all roots of U; i.e., d is invariant under all operations of the Weyl group of U. By the canonical isomorphism of $H^1(T, \boldsymbol{Z})$ with $\operatorname{Hom}(T, \boldsymbol{U}(1))$, the element d gives rise to an homomorphism of T in $\boldsymbol{U}(1)$ which has a unique extension to an homomorphism of U in $\boldsymbol{U}(1)$, also denoted by d. Now let ξ be a principal G-bundle. We extend the principal U-bundle $(E_\xi, E_\xi/U, U)$ by the homomorphism d of U in $\boldsymbol{U}(1)$. We get a principal $\boldsymbol{U}(1)$-bundle over E_ξ/U and the associated line bundle whose first Chern class we also denote by d. Following the notations of 22.6, it is clear that $\pi_\nu{}^*(d)$ is that element of $H^2(E_\xi/T, \boldsymbol{Z})$ which is obtained from the original element $d \in H^1(T, \boldsymbol{Z})$ by the negative transgression in $(E_\xi, E_\xi/T, T)$. Therefore, we may also denote $\pi_\nu{}^*d$ by d.

Now assume moreover that G/U carries an invariant complex structure. Let Ψ be the set of roots of this structure and let Θ be a system of positive roots of U. Then, by (13.7), $\Theta \cup \Psi$ is a positive system of G, to which belongs a positive Weyl chamber. Assume furthermore that d belongs to the closure of this Weyl chamber; i.e., $(d, \alpha) \geqq 0$ for $\alpha \in \Psi$. Let λ be the representation of G with main weight d and let d_ξ be the complex vector bundle over B_ξ associated with the λ-extension of ξ. Now, as in 22.10, we make the hypothesis that B_ξ is a compact almost complex manifold and that E_ξ/U has been given an almost complex structure compatible with the almost complex structure of B_ξ and the complex vector bundle $\hat{\mu}_C$ along the fibres of E_ξ/U arising from the given invariant complex structures on G/U. We have then, using the notations of 22.6, that

$$\mathcal{T}(E_\xi/U, d)^{\natural\mu} = \mathcal{T}(B_\xi, d_\xi). \tag{20}$$

Proof.

$$\mathcal{T}(E_\xi/U, d)^{\natural\mu} = (\pi_\nu{}^*(e^d \cdot \pi_\mu{}^*(\mathcal{T}(B_\xi)) \cdot \mathcal{T}(\hat{\mu}_C)) \cdot \prod_{\alpha\in\Theta} \alpha/(1-e^{-\alpha}))^{\natural\xi}$$
$$= \mathcal{T}(B_\xi)\,(e^d \prod_{\alpha\in\Theta\cup\Psi} \alpha/(1-e^{-\alpha}))^{\natural\xi}.$$

Formula (20) follows then by applying 22.2.

Remarks. (1) Formulas (16) and (20) are closely related to Grothendieck's generalized Riemann-Roch formula (not yet published); compare also with [7b, p. 241].

(2) The representation λ induces a holomorphic map β of G/U into a complex projective space $\boldsymbol{P}_q(\boldsymbol{C})$ such that $d \in H^2(E_\xi/U)$ restricted to G/U equals $\beta^*(e^*)$, where $e^* \in H^2(\boldsymbol{P}_q(\boldsymbol{C}), \boldsymbol{Z})$ is the cohomology class dual to a hyperplane (see 14.4).

23. The A-genus of certain homogeneous spaces. Throughout this paragraph, all cohomology groups are taken with real coefficients and all characteristic classes which occur are regarded as real classes.

23.1. Let $\{\hat{A}_j(p_1, \cdots, p_j)\}$ be the multiplicative sequence of polynomials [19, § 1] with $\frac{1}{2}z^{\frac{1}{2}}/\sinh \frac{1}{2}z^{\frac{1}{2}}$ as characteristic power series. The polynomials $\hat{A}_j$ are related to the A_j introduced in [19, § 1.6] by the equation

$$A_j = 2^{4j}\hat{A}_j.$$

For a real vector bundle ξ, we define the cohomology class $\hat{\mathfrak{A}}(\xi) \in H^{**}(B_\xi)$ as follows:

$$\hat{\mathfrak{A}}(\xi) = \sum_{j=0}^{\infty} \hat{A}_j(p_1(\xi), \cdots, p_j(\xi)).$$

If ξ is the tangent bundle of a differentiable manifold X, then we set $\hat{\mathfrak{A}}(\xi) = \mathfrak{A}(X)$. The genus $\hat{A}(X)$ of a compact oriented differentiable manifold X is given by

$$\hat{A}(X) = \hat{\mathfrak{A}}(X)[X].$$

$\hat{A}(X)$ vanishes if the dimension of X is not divisible by 4. For $\dim X = 4k$, we have

$$\hat{A}(X) = \hat{A}_k(p_1(X), \cdots, p_k(X))[X],$$

and, obviously, $A(X) = 2^{4k}\hat{A}(X)$, where $A(X)$ is the genus corresponding to the power series $2z^{\frac{1}{2}}/\sinh 2z^{\frac{1}{2}}$, and which is called the A-genus of X. If X is almost complex with vanishing first Chern class, then its Todd genus equals its $\hat{A}$-genus; see 22.1 and [19, p. 15].

23.2. Let G be a compact connected Lie group, T a maximal torus of G and U a closed connected subgroup of G containing T. Choose an ordering $\mathcal{S}$ (2.4), let Θ be the set of those roots which are positive with respect to $\mathcal{S}$ and belong to U, and let Ψ be the set of positive complementary roots. Orient U/T and G/T by the invariant complex structures with root systems Θ and $\Theta \cup \Psi$ respectively. We orient G/U by its Euler class using Ψ (see 22.9). Then, in the fibre bundle $(G/T, G/U, U/T)$, the orientations of G/U and and U/T induce that of G/T. Let ξ be a principal G-bundle. We adhere now strictly to the notations given in 22.6. Consider the fibre bundle

$$\mu = (E_\xi/U, B_\xi, G/U, \pi_\mu).$$

We wish to calculate the value of $\hat{A}(G/U)$ and to investigate under which conditions the sequence $\{\hat{A}_j\}$ behaves strictly multiplicatively (21.3) in μ. Let $\hat{\mu}$ be the real vector bundle along the fibres of μ. Then, by 10.7,

$$\pi_\nu^{**}\hat{\mathfrak{A}}(\hat{\mu}) = \prod_{\alpha \in \Psi} \alpha/(2\sinh(\alpha/2))$$

and we get, by the proposition in 22.6, that

$$\hat{\mathfrak{A}}(\hat{\mu})^{\natural\mu} = (\prod_{\beta \in \Theta} \beta/(1 - e^{-\beta}) \prod_{\alpha \in \Psi} \alpha/(2\sinh(\alpha/2)))^{\natural\xi}.$$

If we write s for the sum of all $\alpha \in \Theta$, then

$$\hat{\mathfrak{A}}(\hat{\mu})^{\natural\mu} = (e^{\frac{1}{2}s} \prod_{\alpha \in \Theta \cup \Psi} \alpha/(2\sinh(\alpha/2)))^{\natural\xi}.$$

Let a be the sum of all roots in $\Theta \cup \Psi$. Since $\Theta \cup \Psi$ is a positive system of roots for G and since G/T is oriented by the invariant complex structure

having $\Theta \cup \Psi$ as its set of roots, we get, in virtue of 22.2, that

$$\pi_\xi^{**}(\hat{\mathfrak{a}}(\hat{\mu})^{\natural\mu}) = E(s/4\pi(-1)^{\frac{1}{2}})/E(a/4\pi(-1)^{\frac{1}{2}}). \tag{1}$$

The genus $\hat{A}(G/U)$ is given by the constant term on the right side of the preceding equation which, by 22.3 (4), is also equal to $(s^m/2^m m!)[G/T]$, where $m = \dim_C(G/T)$. Thus, by 22.4 (7),

$$\hat{A}(G/U) = \prod_{\beta \in \Theta \cup \Psi} (s,\beta)/(a,\beta). \tag{2}$$

Now assume that U is the centralizer of a toral subgroup of G and that Ψ is the set of roots of an invariant complex structure on G/U. Then $a - s$ represents the first Chern class of G/U. The element $a - s$ is orthogonal to all roots of Θ (see 14.2 and 14.8). Therefore, $(s,\beta) = (a,\beta)$ for all $\beta \in \Theta$ and thus, by (2),

$$\hat{A}(G/U) = \prod_{\beta \in \Psi} (s,\beta)/(a,\beta). \tag{3}$$

23.3. THEOREM. *Let G be a compact connected Lie group, T a maximal torus of G and U a closed connected subgroup of G containing T. Choose an ordering $\mathcal{S}$ and let Θ be the set of those roots which are positive with respect to $\mathcal{S}$ and belong to U. Let s denote the sum of all $\alpha \in \Theta$. Then the following holds:*

i) *The genus $\hat{A}(G/U)$ vanishes if and only if s is a singular element.*

ii) *If ξ is a principal G-bundle and $\hat{A}(G/U) = 0$, then the sequence $\{\hat{A}_j\}$ is strictly multiplicative in $(E_\xi/U, B_\xi, G/U)$. In particular, if B_ξ is a compact orientable differentiable manifold and ξ a differentiable bundle, then $\hat{A}(G/U) = 0$ implies that $\hat{A}(E_\xi/U) = 0$ also.*

iii) *If $\hat{A}(G/U)$ is not zero, then U is the centralizer of a toral subgroup of G;* i. e., *G/U is homogeneous algebraic* (§ 14). *In particular, $\hat{A}(G/U)$ vanishes if the second Betti number of G/U is zero.*

iv) *If ξ is the universal principal G-bundle and $U \neq G$, then $\{\hat{A}_j\}$ is strictly multiplicative in $(E_\xi/U, B_\xi, G/U)$ if and only if $\hat{A}(G/U) = 0$.*

Proof of i) *and* ii). The statement i) follows from formula (2). If s is singular, then $E(s/4\pi(-1)^{\frac{1}{2}}) = 0$ (see 3.2). Thus, ii) follows from i) and formula (1).

The proof of iii) will be preceded by the following lemma.

23.4. LEMMA. *If G is compact, connected, and semi-simple, if T is a maximal torus of G, and if U $(U \neq G)$ is a closed connected semi-simple*

subgroup of G which contains T, then the sum s of all roots of U which are positive with respect to a given ordering $\mathcal{S}$ on $V_T{}^*$ is singular.

Proof. It is enough to prove the lemma for the case that U is a maximal connected subgroup of G, i.e., U is not contained in a closed connected subgroup of G different from U and G. In this case, we have ([7, p. 205], compare also 10.1)

$$G/U \cong (G_1/U_1) \times (G_2/U_2) \times \cdots \times (G_k/U_k),$$

where G_i is simple, rank $U_i = \operatorname{rank} G_i$, and U_i is a maximal connected subgroup of G_i. The lemma holds for G/U if it is true for at least one of the factors. Thus it suffices to prove the lemma for the case G simple and U a maximal connected subgroup of G. These spaces G/U were listed in [7, p. 219], see also 13.3. Because of i), it suffices to prove the lemma for one ordering on $V_T{}^*$, for then it is proved for all orderings on $V_T{}^*$. The proof will proceed by checking the various cases with G simple and U maximal.

If $G = \boldsymbol{B}_l$ and $U = \boldsymbol{B}_i \times \boldsymbol{D}_{l-i}$ $(0 \leqq i \leqq l-2)$, the positive roots of U with respect to a suitable ordering and a suitable maximal torus are

$$\pm x_r + x_t \ (1 \leqq r < t \leqq i), \ \pm x_r + x_t \ (i+1 \leqq r < t \leqq l), \ x_r \ (1 \leqq r \leqq l).$$

The sum s of these roots is

$$\sum_{j=1}^{i} (2j-1)x_j + 2\sum_{j=1}^{l-i} (j-1)x_{i+j}$$

which is orthogonal to the root x_{i+1}, and thus s is singular.

If $G = \boldsymbol{C}_l$ and $U = \boldsymbol{C}_i \times \boldsymbol{C}_{l-i}$, the positive roots of U with respect to a suitable ordering are (16.4)

$$\pm x_r + x_t \ (1 \leqq r < t \leqq i), \ \pm x_r + x_t \ (i+1 \leqq r < t \leqq l), \ 2x_r \ (1 \leqq r \leqq l).$$

The sum s of these roots is $2\sum_{j=1}^{i} jx_j + 2\sum_{j=1}^{l-i} jx_{i+j}$ which is orthogonal to the root $-x_1 + x_{i+1}$, and thus s is singular. Next we check $\boldsymbol{F}_4/\boldsymbol{B}_4$ and $\boldsymbol{G}_2/\boldsymbol{A}_1 \times \boldsymbol{A}_1$. In these cases, one can choose a set of complementary roots containing for each complementary root α exactly one of the roots α, $-\alpha$ and such that the sum of all roots of this set is 0 (see 18.3 and 19.2). But then it is an immediate consequence of 4.4 that s is singular. The space $\boldsymbol{G}_2/\boldsymbol{A}_2$ has dimension 6 (in fact, it is the 6-sphere). Thus $\hat{A}(\boldsymbol{G}_2/\boldsymbol{A}_2) = 0$, and the lemma is correct in this case by i).

If G is simple and U maximal, one can choose orderings $\mathcal{S}$ and $\mathcal{S}'$ on $V_T{}^*$ such that each root of U simple with respect to $\mathcal{S}$ is a root of G which

is either simple with respect to $\mathfrak{S}'$ or equals the negative dominant root of G with respect to $\mathfrak{S}'$ (see [7]). If $G = \boldsymbol{D}_l$, $\boldsymbol{E}_6$, $\boldsymbol{E}_7$, $\boldsymbol{E}_8$, then all $\mathfrak{S}'$-simple roots of G and the corresponding dominant root of G have equal lengths and thus all simple roots of U with respect to the ordering $\mathfrak{S}$ have all the same length ρ in the Killing metric of G. Then the sum s of all roots of U which are positive with respect to $\mathfrak{S}$ has a representative contravariant vector lying in the principal diagonal of the $\mathfrak{S}$-positive Weyl chamber of U [25a, p. 221], since $(s,\beta) = (\beta,\beta)$ for each $\mathfrak{S}$-simple root β of U, by 3.1. According to [25a, Théorème 7], the principal diagonal contains only singular vectors, and thus s is singular.

It remains to check our lemma for the spaces $\boldsymbol{F}_4/\boldsymbol{A}_1 \times \boldsymbol{C}_3$ and $\boldsymbol{F}_4/\boldsymbol{A}_2 \times \boldsymbol{A}_2$. The Schläfli diagram of $\boldsymbol{F}_4$ (including the dominant root) is

$$\begin{array}{ccccccccc} 1 & & 1 & & 2 & & 2 & & 2 \\ \bullet & - & \bullet & = & \bullet & - & \bullet & - & \bullet \\ \phi_1 & & \phi_2 & & \phi_3 & & \phi_4 & & -\phi \end{array}$$

where the ϕ_i are the $\mathfrak{S}'$-simple roots of $\boldsymbol{F}_4$ and where $\phi = 2\phi_1 + 4\phi_2 + 3\phi_3 + 2\phi_4$ is the $\mathfrak{S}'$-dominant root [25a]. The integers 1, 2 indicate the values of (ϕ_i, ϕ_i) and (ϕ, ϕ).

The subgroup $U = \boldsymbol{A}_1 \times \boldsymbol{C}_3$ is represented by the following diagram which indicates the $\mathfrak{S}$-simple roots of U.

$$\begin{array}{ccccccc} 1 & & 1 & & 2 & & 2 \\ \bullet & - & \bullet & = & \bullet & & \bullet \\ \phi_1 & & \phi_2 & & \phi_3 & & -\phi \end{array}$$

By an easy calculation, we get for the sum s of all $\mathfrak{S}$-positive roots of U

$$s = 4\phi_1 + 6\phi_2 + 3\phi_3 - 2\phi_4$$

which is orthogonal to the root $\phi_1 + 2\phi_2 + 2\phi_3 + \phi_4$. Thus s is singular.

Finally, we consider $\boldsymbol{F}_4/\boldsymbol{A}_2 \times \boldsymbol{A}_2$. This space is almost complex (13.3) with vanishing Todd genus (22.8). Since the second Betti number of $\boldsymbol{F}_4/\boldsymbol{A}_2 \times \boldsymbol{A}_2$ is zero, also the $\hat{A}$-genus vanishes (23.1) and thus the lemma is true in this case by (i).

The proof of the lemma is completed.[2]

23.5. *Proof of* iii). The proof proceeds by induction on the dimension of G/U. Assume iii) is proved for U', G' with $\dim G'/U' < n$. We prove it now for U, G with $\dim G/U = n$. If Q is the center of G, then G/U

[2] (Added in proof). Another proof of this lemma will be given in a forthcoming paper of the authors.

$=(G/Q)/(U/Q)$ and if U/Q is the centralizer of a toral subgroup in G/Q, then the same holds for U in G, and conversely. Thus, in proving iii) for U, G with $\dim G/U = n$, we may assume that G is semi-simple. Suppose $\hat{A}(G/U) \neq 0$. Then by i) and 23.4, the subgroup U is not semi-simple. Let T' be the identity component of its center and V the centralizer of T'. Then V is connected. $V \neq G$, since G is semi-simple. Thus $U \subset V \subsetneq G$. We have the fibre bundle $(G/U, G/V, V/U)$ and $\hat{A}(V/U) \neq 0$ by ii). By the induction hypothesis, U is the centralizer of T' in V; but then $U = V$.

23.6. *Proof of* iv). Let ξ be the universal principal G-bundle. It follows immediately from formula (1) in 23.2 that the sequence $\{\hat{A}_j\}$ is strictly multiplicative in $(E_\xi, B_\xi, G/U)$ if and only if the function $E(s)\cdot E(a)^{-1}$, which is defined on V_T, is a constant (see 3.2). This happens in the following two cases and only then.

a) $E(s)$ is identically 0. b) $E(s) = \pm E(a)$.

We shall show that b) is impossible, if $U \neq G$. If b) holds, then s is not singular and U is the centralizer of a toral subgroup of G, according to i) and iii). From b), we infer more precisely that s is a transform of a under the Weyl group of G; i.e., $s = w(a)$ for some $w \in W(G)$. Now we can define a new ordering by letting the element $x \in V_T{}^*$ be positive if $(s, x) > 0$. Since $s = w(a)$, we conclude that s equals the sum of all roots of G which are positive in this ordering. Since $(s, \beta) > 0$ for all $\beta \in \Theta$ (notations of 23.3), all $\beta \in \Theta$ are positive in the new ordering. Since s is the sum of all roots in Θ, we infer that the sum of all complementary roots positive in the new ordering is zero which is impossible if $U \neq G$. Therefore $\{\hat{A}_j\}$ is strictly multiplicative in $(E_\xi/U, B_\xi, G/U)$ if and only if a) holds, but this is the case if and only if s is singular (3.2). In virtue of 23.3, i), the element s is singular if and only if $\hat{A}(G/U)$ vanishes. This completes the proof.

23.7. *Remarks.*

1) As a corollary of 23.3, i), we mention that s is singular if the real dimension of G/U is not divisible by 4. Thus s can only be non-singular if G/U is homogeneous algebraic of even complex dimension, see 23.3, iii).

2) In view of 23.3, ii), one might formulate the following *conjecture*: Let ξ be a bundle for which F_ξ is a compact oriented differentiable manifold and G_ξ is a group of differentiable homeomorphisms of F_ξ. If $\hat{A}(F_\xi) = 0$, then $\{\hat{A}_j\}$ is strictly multiplicative in ξ. (For the notations see 21.1-21.3.)

3) If the first Chern class of a compact almost complex manifold X vanishes, then $\hat{A}(X)$ is equal to the Todd genus of X. Taking this into account, 23.3, iii) is in agreement with 13.2 and 22.8.

4) In the proof of Lemma 23.4, we used the theorem of de Siebenthal on the principal diagonal. de Siebenthal proved his theorem by "checking all cases." There exists a general proof of it (A. Borel, unpublished).

24. Applications to simply connected algebraic homogeneous spaces.

24.1. Let X be a non-singular n-dimensional projective manifold, whose cohomology classes with respect to complex coefficients of type (p,q) vanish if $p \neq q$. Then the $h^{p,q}$ of X satisfy (see for instance [19]):

$$\chi^p(X) = \sum_{q=0}^{n} (-1)^q h^{p,q} = (-1)^p h^{p,p},$$
$$\chi^p(X) = (-1)^p \sum_{r+s=2p} h^{r,s} = (-1)^p b_{2p}, \tag{1}$$

where b_i is the Betti number of X in the real dimension i; it vanishes if i is odd. From (1) and [19, § 21.3], we conclude

$$T_y(X) = \sum_{p=0}^{n} (-y)^p b_{2p}. \tag{2}$$

For $y = 1$ (respectively $y = -1$), $T_y(X)$ is equal to the index $\tau(X)$ (respectively the Euler number $E(X)$) of X ([19], pp. 84, 122); hence

$$\tau(X) = \sum_{p=0}^{n} (-1)^p b_{2p}, \qquad E(X) = \sum_{p=0}^{n} b_{2p}. \tag{3}$$

24.2. Let G be a compact connected Lie group, T a maximal torus, and U the centralizer of a toral subgroup of T. Let $\mathcal{J}$ be an invariant complex structure on G/U, Ψ its root system and Θ a system of positive roots of U. Then (13.7), $\Theta \cup \Psi$ is a positive system of roots of G. The complex manifold G/U (with the structure $\mathcal{J}$) is projective and satisfies the assumptions of 24.1 (see 14.4, 14.10). It follows then from (2) and 22.7, in the notations of 22.7, that

$$b_{2p}(G/U) = k^p(G/U, \Psi, \Theta). \tag{4}$$

As was recalled in 2.7, the map $w \to w(\Theta \cup \Psi)$ is a 1-1 correspondence between the Weyl group $W(G)$ of G and the systems of positive roots. Let $W(G/U, \Psi, \Theta)$ be the set of those elements in $W(G)$ for which $\Theta \subset w(\Theta \cup \Psi)$. Each *right* coset $w(U) \cdot w$ of $W(G)$ modulo $W(U)$ contains at most one

element of $W(G/U, \Psi, \Theta)$, since only the identity of $W(U)$ transforms Θ onto Θ. Moreover, given $w \in W(G)$, the system $w(\Theta \cup \Psi)$ contains a system Θ' of positive roots of U; hence, if u is the element of $W(U)$, carrying Θ' onto Θ, we have $u \cdot w \in W(G/U, \Psi, \Theta)$. Thus $W(G/U, \Psi, \Theta)$ is a system of representatives for the right cosets of $W(G)$ modulo $W(U)$.

Given $w \in W(G)$, let $\mu(w)$ be the number of elements in $w(\Theta \cup \Psi) \cap (-\Psi)$. Then, clearly, $k^p(G/U, \Psi, \Theta)$ is the number of elements in $W(G/U, \Psi, \Theta)$ for which $\mu(w) = p$. Since Ψ is invariant under $W(U)$, (13.4, remark), we have $\mu(w) = \mu(w')$ if w and w' belong to the same right coset of $W(G)$ modulo $W(U)$. By (4) and 13.7, we have the:

24.3. THEOREM. *Let U be the centralizer of a torus in the compact connected Lie group G. Let $\mathcal{S}$ be an ordering of the roots of G for which the set Ψ of positive complementary roots is closed. For $w \in W(G)$, let $\mu(w)$ be the number of positive roots whose image under w is a negative complementary root. Then we have, with $2n = \dim G/U$:*

$$(5) \qquad \begin{aligned} \sum_{p=0}^{n} b_{2p} t^{2p} &= (\operatorname{ord} W(U))^{-1} \sum_{w \in W(G)} t^{2\mu(w)}, \\ \tau(G/U) = \sum_{p=0}^{n} (-1)^p b_{2p} &= (\operatorname{ord} W(U))^{-1} \sum_{w \in W(G)} (-1)^{\mu(w)}, \end{aligned}$$

where $\tau(G/U)$ is the index of G/U, and b_{2p} its $2p$-th Betti number.

24.4. It follows in particular that $b_{2p}(G/T)$ (T maximal torus of G) equals the number of elements of $W(G)$ for which $w(\Psi)$ contains exactly p negative roots. Therefore, in the notations of 2.6, we have

$$\sum_{p=0}^{n} b_{2p}(G/T) t^{2p} = \sum_{w \in W(G)} t^{2s(w)}.$$

Theorem 24.3 was proved independently by R. Bott (Bull. Soc. Math. France 84 (1956), 251-281) in a slightly different formulation. 24.4 was also proved by C. Chevalley by means of a cellular decomposition (Tohoku Math. Journal 7 (1955), 14-66). The general case could also be read off from the cellular decomposition mentioned in [5].

24.5. *Kodaira's vanishing theorem.* Let X be a compact connected Kählerian manifold, n its complex dimension, and F a holomorphic complex line bundle over X. The bundle F is said to be negative of order $\geqq k$ if its first Chern class $c_1(F)$ can be represented by a closed real $(1,1)$-form ω of class C^∞ which, around every point $x \in X$, can be written in the form

$$\omega = i \sum g_{\alpha\bar{\beta}} dz_\alpha \wedge d\bar{z}_\beta$$

where $(g_{\alpha\bar{\beta}})$ is a hermitian matrix with at least k negative eigenvalues. In particular, F is negative of order $\geqq n$ if and only if it is negative in the sense of Kodaira, that is, if and only if F^{-1} is positive in the sense of Kodaira. In [22], Kodaira has shown that *if F is negative, then the cohomology groups $H^q(X,F)$ of X with respect to the sheaf of germs of holomorphic sections of F vanish for $q < \dim_{\mathbf{C}} X$.* By Serre's duality theorem, this is equivalent to the following statement: *Let K be the canonical bundle of X. If $F \otimes K^{-1}$ is positive, then $H^q(X,F) = 0$ for $q > 0$.*

Bott [7b, p. 231] has given a generalization of the first theorem in the case $q = 0$: *if F is negative of order $\geqq 1$, then $H^0(X,F) = 0$, that is, F does not admit a not identically zero holomorphic cross section.*

Remark. Bott formulates his theorem in a slightly different fashion; but, if one takes into account the lemma in [22, p. 1271], one gets Bott's theorem in the above form.

24.6. We keep the notations of 24.1 and 24.2. Since $H^{0,1}(G/U) = H^{0,2}(G/U) = 0$, by 14.10, the map assigning to a holomorphic line bundle over G/U its first Chern class defines an isomorphism between the group of isomorphism classes of line bundles and $H^2(G/U, \mathbf{Z})$. The negative transgression defines a homomorphism of the group A of weights which are orthogonal to the roots of U onto $H^2(G/U,\mathbf{Z})$ by 14.2. For any weight, we define $H^i(G/U,d)$ as the i-th cohomology group of G/U with respect to the sheaf of germs of holomorphic sections of a complex bundle with first Chern class d. $\chi(G/U,d)$ will denote the alternating sum of the dimensions of the $H^i(G/U,d)$.

24.7. THEOREM. *Let U be the centralizer of a torus in G, Ψ be the set of roots of an invariant complex structure on G/U, and Θ a set of positive roots for U. Let d be a weight orthogonal to the roots of U. If $(d,b) \geqq 0$ for all $b \in \Psi$, then $H^i(G/U,d) = 0$ $(i > 0)$ and $\dim_{\mathbf{C}} H^0(G/U,d)$ equals $T(G/U,d)$, which is the degree of the irreducible representation of $\tilde{G}$* (see 3.3) *with main weight d (in the ordering which has $\Theta \cup \Psi$ as positive roots). If $(d,b) < 0$ for at least one $b \in \Psi$, then $H^0(G/U,d) = 0$.*

The last assertion follows from Bott's theorem (24.5) and 14.6. Let c_1 be the first Chern class of G/U. Then $(c_1,b) > 0$ for $b \in \Psi$ by 14.8, and $(d,b) \geqq 0$ for $b \in \Psi$ implies $(d + c_1, b) > 0$. Since $c_1 = -c_1(K)$, the vanishing of $H^i(G/U,d)$, $(i > 0)$, follows then from 14.6 and 24.5.

Assume G/T and U/T to be endowed with the invariant complex structures having as root systems $\Theta \cup \Psi$ and Θ respectively. Then (14.3),

$(G/T, G/U, U/T, \nu)$ is a complex analytic fibering; we have by 22.8 and 22.10

$$T(G/U, d) = T(G/T, d), \tag{6}$$

and, therefore, by Riemann-Roch

$$\chi(G/U, d) = \chi(G/T, d). \tag{7}$$

Since $H^i(G/U, d) = H^i(G/T, d) = 0$ for $i > 0$, we get

$$\dim_C H^0(G/U, d) = T(G/T, d),$$

and the remaining assertion of the theorem follows from 22.4.

Remarks. (1) Assume that $U = T$. Let $d \in H^2(G/T, \boldsymbol{Z})$ be such that $d + (c_1/2)$ is in the closure of the positive Weyl chamber, but not inside; therefore it is singular, $(d, b) < 0$ for at least one positive root b, and $(d + c_1, b) > 0$ for all positive roots b. By 14.6 and 24.5, it follows that *all* cohomology groups $H^i(G/T, d)$ vanish, in agreement with the fact (22.3(5)) that $T(G/T, d) = \chi(G/T, d) = 0$ if $d + (c_1/2)$ is singular.

(2) If the weight d is orthogonal to the roots of U, the element $d \in H^2(G/T, \boldsymbol{Z})$ is the first Chern class of a line bundle which is the image under ν^* of a line bundle on G/U with first Chern class $d \in H^2(G/U, \boldsymbol{Z})$. Since $H^{p,q}(U/T) = 0$ for $p \neq q$ (14.10), one can deduce by a spectral argument applied to the fibering $(G/T, G/U, U/T, \nu)$ that, more generally than in the proof of 24.7, ν^* induces an isomorphism of $H^i(G/U, d)$ onto $H^i(G/T, d)$ for all i and all d.

24.8. We assume here that G is semi-simple. Then $H^2(G/T, \boldsymbol{Z})$ is isomorphic to the group of weights of G.

The projective space associated to the vector space $H^0(G/T, d)$ can be identified with the complete linear system of all positive divisors whose homology class is dual to d. Thus the preceding results on $\dim H^0(G/T, d)$ are also consequences of the results of [7a] quoted in 14.4.

Bott [7b] has proved the following theorem, which had been conjectured by the authors in view of 22.2 and 24.7:

THEOREM (Bott). *Let d be a weight. Then all groups $H^i(G/T, d)$ vanish if and only if $d + (c_1/2)$ is singular. If $d + (c_1/2)$ is regular and if w is the unique element of $W(G)$ which brings $d + (c_1/2)$ into the positive Weyl chamber, then $H^i(G/T, d)$ is zero if $i \neq s(w)$, and is equal to the degree of the irreducible representation $\bar{G}$ with main weight $w(d + (c_1/2)) - (c_1/2)$ if $i = s(w)$ (see 2.6 for $s(w)$).*

24.9. *Degrees of embeddings.* We follow the preceding notations. Let d be a weight orthogonal to all roots of U for which moreover $(d,b)>0$ for all $b\in\Psi$. Let Γ be the representation with main weight d and $\check{\Gamma}$ the contragredient representation. G/U is *strictly* associated (14.4) to Γ, and $\check{\Gamma}$ induces an embedding j of G/U in the complex projective space $\boldsymbol{P}_q(\boldsymbol{C})$, where $q+1$ is the degree of the representation Γ. If $e^*=H^2(\boldsymbol{P}_q(\boldsymbol{C}),\boldsymbol{Z})$ is dual to a hyperplane of $\boldsymbol{P}_q(\boldsymbol{C})$, then $j^*(e^*)=d$ (d regarded now as element of $H^2(G/U,\boldsymbol{Z})$) and the value of the cohomology class d^n ($n=\dim_C G/U$) on the fundamental cycle of G/U is the degree of the embedding in the sense of algebraic geometry. The following formula is clear for an arbitrary $d\in H^2(G/U,\boldsymbol{R})$

$$d^n[G/U]=n!\lim_{r\to\infty} r^{-n}T(G/U,rd).$$

Let a be the sum of all roots in $\Theta\cup\Psi$, then (6) and 22.3(4) and 22.4(7) give

$$T(G/U,rd)=\prod_{c\in\Theta}(rd+a/2,c)/(a/2,c)\cdot\prod_{b\in\Psi}(rd+a/2,b)/(a/2,b).$$

Since $(d,c)=0$ for $c\in\Theta$, the first product equals 1. Passing to the limit yields

$$(8)\qquad d^n[G/U]=n!\prod_{b\in\Psi}(d,b)/(a/2,b)\qquad\text{for } d\in H^2(G/U,\boldsymbol{R}).$$

24.10. THEOREM. *Let G be a compact connected Lie group, T a maximal torus of G and U the centralizer of a toral subgroup of T. Endow G/U with an invariant complex structure, and let Ψ be the set of its roots. Choose an ordering $\mathcal{S}$ on V_T for which Ψ is the set of all positive complementary roots. Let a be the sum of all positive roots. Let d be a weight orthogonal to the roots of U and for which $(d,b)>0$ for all $b\in\Psi$. The contragredient representation of the irreducible representation of $\tilde{G}$ (3.3) with main weight d induces an embedding of G/U in a complex projective space (14.4). The degree of this embedding in the sense of algebraic geometry is*

$$(9)\qquad d^n[G/U]=n!\prod_{b\in\Psi}(d,b)/(a/2,b),\qquad (n=\dim_C G/U).$$

24.11. As an example, we take $G=\boldsymbol{U}(4)$ and $U=\boldsymbol{U}(2)\times\boldsymbol{U}(1)\times\boldsymbol{U}(1)$. In 13.9, two invariant complex structures $\mathcal{J}_1$, $\mathcal{J}_2$ on G/U were defined. We shall calculate the number $c_1{}^5[G/U]$ with respect to these two structures. Let $a^{(1)}$ (respectively $a^{(2)}$) be the sum of the positive roots with respect to the ordering $\mathcal{S}_1$ (respectively $\mathcal{S}_2$) defined in 13.9. We have

$$a^{(1)}=3x_4+x_1-x_2-3x_3,\qquad a^{(2)}=3x_1+x_2-x_3-3x_4.$$

The first Chern classes and the roots of these two structures have been given in 13.9. With respect to the coordinates x_i, the metric in the universal covering V_T of the maximal torus of $U(4)$ is the usual euclidean metric. Thus, in the formulas (8), (9), the scalar product is the ordinary one, and, by a straightforward computation, the Chern number $c_1{}^5[G/U]$ of G/U with respect to $\mathscr{B}_1$ (respectively $\mathscr{B}_2$) is 4860 (respectively 4500). Therefore we get an example of two 5-dimensional algebraic varieties which are C^∞-differentiably homeomorphic, but have different Chern numbers.

Chapter VII. Genera Defined by Pontrjagin Classes.

In this chapter, a real number s is said to be an integer exc 2, or integral exc 2, if there exists an integer k such that $2^k \cdot s$ is an integer. Analogously, a real cohomology class x is integral exc 2 if x, multiplied by a suitable power of 2, is the image of an integral cohomology class under the coefficient homomorphism induced by $\mathbf{Z} \to \mathbf{R}$.

25. The integrality of the A-genus.

25.1. Let $\{L_j(p_1, \cdots, p_j)\}$ and $\{A_j(p_1, \cdots, p_j)\}$ be the multiplicative sequences [19, § 1] with $z^{\frac{1}{2}}/\mathrm{tgh}\, z^{\frac{1}{2}}$ and $2z^{\frac{1}{2}}/\sinh 2z^{\frac{1}{2}}$ respectively as characteristic power series. The polynomials A_k have rational coefficients which, when written as quotients of relatively prime integers, do not contain the factor 2 in their denominators. It suffices to prove this for the coefficients a_k of the power series $2z^{\frac{1}{2}}/\sinh 2z^{\frac{1}{2}}$. The coefficient of z^k $(k \geqq 1)$ in this series is

$$a_k = (-1)^k 2^{2k+1}(2^{2k-1} - 1) B_k/(2k)\,!$$

and, by elementary number theory, $(2k)\,!$ is not divisible by 2^{2k}, whereas by von Staudt's theorem, the Bernoulli number B_k contains 2 exactly to the first power in its denominator, which proves the desired result.

25.2. If X is a compact oriented differentiable manifold, then the genera $L(X)$, $A(X)$, $\hat{A}(X)$ are defined (21.2, 23.1). They are rational numbers which vanish if the dimension of X is not divisible by 4. We have

$$A(X) = 2^{4k}\hat{A}(X) \qquad \text{for } \dim X = 4k.$$

$A(X)$ may be written with an odd denominator; by [19, Haupsatz 8.2.2], the rational number $L(X)$ equals the index $\tau(X)$ and thus is an integer. In this paragraph, we wish to prove in particular that the A-genus $A(X)$ is also an integer or, equivalently, that $\hat{A}(X)$ is integral exc 2.

For a compact almost complex manifold X with Chern classes $c_i \in H^{2i}(X, \boldsymbol{Z})$ and for elements $d_1, \cdots, d_s \in H^2(X, \boldsymbol{R})$, we define the virtual Todd genus as in [19, § 11] by the formula

$$(1) \qquad T(d_1, \cdots, d_s)_X = ((1-e^{-d_1}) \cdots (1-e^{-d_s}) \sum_{j=0}^{\infty} T_j(c_1, \cdots, c_j))[X].$$

This virtual Todd genus is a real number.

For $d \in H^2(X, \boldsymbol{R})$ the number $T(X, d)$ is defined by the formula

$$(2) \qquad T(X, d) = (e^d \sum_{j=0}^{\infty} T_j(c_1, \cdots, c_j))[X], \qquad \text{(see 22.1)}.$$

By [19, Satz 14.3.2], the Todd genus $T(X) = T(X, 0)$ is an integer exc 2 and the virtual Todd genus $T(d_1, \cdots, d_s)_X$ is integral exc 2 if $d_1, \cdots, d_s$ are images of integral cohomology classes. We have

$$T(X, d) = T(X) - T(-d)_X$$

and thus $T(X, d)$ is also integral exc 2 if d is the image of an integral class. We give now a slight generalization of these results.

25.3. PROPOSITION. *If the elements $d, d_1, \cdots, d_s$ of $H^2(X, \boldsymbol{R})$, (X compact almost complex), are integral* exc 2, *then $T(X, d)$ and the virtual Todd genus $T(d_1, \cdots, d_s)_X$ are integral* exc 2.

By (1) and (2), it is sufficient to prove that $T(X, d)$ is integral exc 2 if $2^k d$ is the image of an integral class for some positive integer k. This statement will be proved by induction on k. It is proved already for $k = 0$, and we assume it to be true for $k - 1$. We have

$$e^d = (1 - (1 - e^{-2d}))^{-\frac{1}{2}},$$

and therefore

$$T(X, d) = \left(\sum_{r=0}^{\infty} (-1)^r \binom{-\frac{1}{2}}{r} (1 - e^{-2d})^r \cdot \sum_{j=0}^{\infty} T_j(c_1, \cdots, c_j) \right) [X].$$

The coefficients $(-1)^r \binom{-\frac{1}{2}}{r} = 2^{-2r} \binom{2r}{r}$ are integers exc 2. If $2^k d$ is the image of an integral class, we see that $T(X, d)$ is a finite linear combination, with integers exc 2 as coefficients, of numbers $T(X, f)$, where f runs through certain elements of $H^2(X, \boldsymbol{R})$ for which $2^{k-1} f$ is the image of an integral class. By the induction assumption, it is therefore an integer exc 2.

The following theorem will include the integrality of the A-genus (25.2).

25.4. THEOREM. *Let X be a compact oriented differentiable manifold with the Pontrjagin classes $p_j \in H^{4j}(X, \boldsymbol{Z})$. Let the element d of $H^2(X, \boldsymbol{R})$*

be integral exc 2. *Then the number* $\hat{A}(X,d)$ *defined by*

$$\hat{A}(X,d) = (e^d \sum_{j=0}^{\infty} \hat{A}_j(p_1,\cdots,p_j))[X]$$

is integral exc 2.

The theorem is trivial if the dimension of X is odd. Therefore we may put $\dim X$ equal to $2q$. Let $\xi = (E, X, \boldsymbol{SO}(2q))$ be the principal tangent bundle of X. Let T be a maximal torus of $\boldsymbol{SO}(2q)$ and $(x_1,\cdots,x_q)$ a base of $H^1(T,\boldsymbol{Z})$, see 10.1. We consider the fibre bundle

$$\zeta = (E/T, X, \boldsymbol{SO}(2q)/T, \pi).$$

Then $\pi^*(\xi)$ is the Whitney sum of q principal $\boldsymbol{U}(1)$-bundles $\xi_1,\cdots,\xi_q$, where ξ_j is the extension of $(E, E/T, T)$ with respect to $t \rightarrow \exp 2\pi i x_j(t)$. The first Chern class of ξ_i is x_i if we regard x_i under the negative transgression of $(E, E/T, T)$ as an element of $H^2(E/T,\boldsymbol{Z})$. Let $a_1,\cdots,a_m$ $(m = q(q-1))$, be the positive roots of $\boldsymbol{SO}(2q)$ with respect to T and an ordering. The a_i are the roots of an invariant integrable almost complex structure (§ 12) on $\boldsymbol{SO}(2q)/T$, to which belongs a complex structure of the vector bundle along the fibres of ζ. Thus the principal bundle η along the fibres of ζ is restricted to $\boldsymbol{U}(m)$ and the corresponding principal $\boldsymbol{U}(m)$-bundle η' is the Whitney sum of m principal $\boldsymbol{U}(1)$-bundles $\eta_1, \eta_2,\cdots,\eta_m$ whose first Chern classes are $a_1,\cdots,a_m$ regarded as elements of $H^2(E/T,\boldsymbol{Z})$.

The principal tangent bundle of E/T is the Whitney sum of $\pi^*\xi$ and η; thus E/T admits an almost complex structure whose principal tangent $\boldsymbol{U}(m+q)$-bundle is the Whitney sum of $\eta_1,\cdots,\eta_m, \xi_1,\cdots,\xi_q$. Hence E/T is an almost complex split manifold [19, § 13.5] with total Chern class

$$c(E/T) = (1+a_1)(1+a_2)\cdots(1+a_m)(1+x_1)(1+x_2)\cdots(1+x_q).$$

By 22.5(11), we get for an arbitrary element $d \in H^2(X,\boldsymbol{R})$,

$$\hat{A}(X,d) = (\pi^*(e^d)\prod_{j=1}^{m} a_j/(1-e^{-a_j})\cdot\pi^*(\sum_{k=0}^{\infty}\hat{A}_k(p_1,\cdots,p_k)))[E/T].$$

Observing that

$$\pi^*(p(\xi)) = p(\pi^*\xi) = (1+x_1^2)(1+x_2^2)\cdots(1+x_q^2)$$

and using the identity $x/(1-e^{-x}) = (\frac{1}{2}x/\sinh\frac{1}{2}x)\cdot\exp(x/2)$, we obtain

$$\pi^*(\sum_{k=0}^{\infty}\hat{A}_k(p_1,\cdots,p_k))$$
$$= \prod_{i=1}^{q}(x_i/2)/\sinh(x_i/2) = e^{-\frac{1}{2}(x_1+\cdots+x_q)}\prod_{i=1}^{q} x_i/(1-e^{-x_i}).$$

Thus we see that

$$\hat{A}(X,d)=T(E/T,\pi^*(d)-\tfrac{1}{2}(x_1+\cdots+x_q)),$$

and this, together with 25.3, proves 25.4.

25.5. THEOREM. *Let* $\eta=(E,X,\boldsymbol{U}(k))$ *be a principal bundle over a compact oriented differentiable manifold* X $(\dim X=2q)$ *and let* p_j *denote the Pontrjagin classes of* X. *Let* $d\in H^2(X,\boldsymbol{R})$ *be integral* exc 2. *Then the number* $\hat{A}(X,d,\eta)$ *defined by*

$$\hat{A}(X,d,\eta)=(e^d\operatorname{ch}(\eta)\cdot\sum_{j=0}^{\infty}\hat{A}_j(p_1,\cdots,p_j))[X]$$

is integral exc 2. (As in 9.1, $\operatorname{ch}(\eta)$ denotes the Chern-character of η).

We consider the associated bundle $\zeta=(E/T,X,\boldsymbol{U}(k)/T,\pi)$ where T is the standard maximal torus of $\boldsymbol{U}(k)$. Let $(x_1,\cdots,x_k)$ be the standard base of $H^1(T,\boldsymbol{Z})$. Then $\pi^*(\eta)$ is the Whitney sum of k principal $\boldsymbol{U}(1)$-bundles whose first Chern classes are $x_1,\cdots,x_k$ if we consider $x_1,\cdots,x_k$ via negative transgression as elements of $H^2(E/T,\boldsymbol{Z})$. We note that

$$\pi^*\operatorname{ch}(\eta)=\operatorname{ch}(\pi^*\eta)=e^{x_1}+e^{x_2}+\cdots+e^{x_k}. \tag{3}$$

Let $a_1,\cdots,a_m$ $(m=k(k-1)/2)$ be the positive roots of $\boldsymbol{U}(k)$ with respect to T and an ordering. By 10.7, the Pontrjagin class $\hat{p}$ of the bundle ζ along the fibres of ζ is given by

$$\hat{p}=\prod_1^m(1+a_i^2) \tag{4}$$

and therefore

$$\sum\hat{A}_j(\hat{p}_1,\cdots,\hat{p}_j)=\prod(a_i/2)/\sinh(a_i/2)=e^{-(a_1+\cdots+a_m)/2}\cdot\prod a_i/(1-e^{-a_i}). \tag{5}$$

The tangent bundle to E/T is the direct sum of $\hat{\zeta}$ and of $\pi^*\sigma$ where σ is the tangent bundle to X (7.6). Thus if p'_i denotes the i-th Pontrjagin class of E/T, we have in view of (5)

$$\pi^*(\sum\hat{A}_j(p_1,\cdots,p_j))\cdot\prod a_i/(1-e^{-a_i})=e^{(a_1+\cdots+a_m)/2}\sum\hat{A}_j(p'_1,\cdots,p'_j). \tag{6}$$

On the other hand, it follows from 22.5(11) that

$$\hat{A}(X,d,\eta)=(\pi^*(e^d\cdot\operatorname{ch}(\eta)\cdot\sum\hat{A}_j(p_1,\cdots,p_j))\cdot\prod a_i/(1-e^{-a_i}))[E/T].$$

Together with (3) and (6), this gives

$$\hat{A}(X,d,\eta)=\sum_i\hat{A}(E/T,\pi^*(d)+x_i+(a_1+\cdots+a_m)/2),$$

and the right hand side is an integer exc 2 by Theorem 25.4.

25.6. *Remarks.* The preceding theorem is the most general integrality theorem we give in this paper. All the theorems of integrality for the Todd genus, etc., [19, § 14.4, 2)] are formal consequences of it: Let X be a compact almost complex manifold of complex dimension q and η a principal $\boldsymbol{U}(k)$-bundle over X. We have $T(X,\eta)=\hat{A}(X,c_1/2,\eta)$. Thus $T(X)$ and $T(X,\eta)$ are integers exc 2. As a consequence, $T_y(X)$ and $T_y(X,\eta)$ are polynomials in y with integers exc 2 as coefficients [19, p. 93, (7), (8)]. The virtual T_y-characteristic $T_y(v_1,\cdots,v_r\,|,\eta)_X$ as defined in [19, p. 95], ($v_1,\cdots,v_r$ are elements of $H^2(X,\boldsymbol{Z})$), is a polynomial of degree $q-r$ in y which can be written as a formal power series in y, the coefficients being finite linear combinations with integral coefficients of polynomials $T_y(X,\xi)$, where ξ runs through certain unitary bundles depending on η, $v_1,\cdots,v_r$. This is purely formal (see also the analogous statement for the χ_y-theory, [19, p. 132]). Thus, $T_y(v_1,\cdots,v_r\,|,\eta)_X$ is also a polynomial with integers exc 2 as coefficients.

The proofs of 25.4 and 25.5 depend mainly on the strictly multiplicative behaviour of $x(1-e^{-x})^{-1}$, and on Proposition 25.3 which we actually would need only for almost complex split manifolds. The theory of Thom enters implicitly in the proof of 25.3 (integrality of virtual indices, see [19, § 9 and end of § 13]).

We do not know how far in 25.5 "integral exc 2" could be replaced by "integral." We can only dare the following *conjectures* which are motivated by the theorem of Riemann-Roch (see [18]). Let X be a compact oriented differentiable manifold and η a principal $\boldsymbol{U}(k)$-bundle over X.

1) *Let w_2 denote the second Stiefel-Whitney class of X, ($w_2\in H^2(X,\boldsymbol{Z}_2)$). If $d\in H^2(X,\boldsymbol{Z})$ reduced* mod 2 *is w_2, then $\hat{A}(X,d/2,\eta)$ is an integer.*

2) *If $w_2=0$ and* $\dim X\equiv 4 \pmod 8$, *then $\hat{A}(X)$ is an even integer.*

2*) *If $w_2=0$,* $\dim X\equiv 4 \pmod 8$ *and if the structural group of η can be reduced to $\boldsymbol{SO}(k)$, then $\hat{A}(X,0,\eta)$ is an even integer.*

These conjectures would be generalizations of Rohlin's theorem [24] that the Pontrjagin number $p_1[X]$ is divisible by 48 if $\dim X=4$ and $w_2=0$. Rohlin's theorem goes over into conjecture 2 fro $\dim X=4$.[3]

25.7. *Examples.* Putting the value 0 for d in 25.4 yields that $\hat{A}(X)$

[3] (Added in proof). A proof of (1), using the integrality of the Todd genus recently proved by Milnor (yet unpublished) will be given in the paper mentioned in footnote 2). For a different approach which proves (1) and (2*), see F. Hirzebruch, Séminaire Bourbaki, Exposé 177, Febr. 1959.

is integral exc 2 or, equivalently, that the $\hat{A}$-genus of X (see 25.2) is an integer. This is non-trivial only if the dimension of X is divisible by 4. For $\dim X = 8$, we get [19, p. 14]

$$(5) \qquad (-4p_2 + 7p_1^2)[X] \equiv 0 \pmod{45}.$$

The integrality of the L-genus (index) gives

$$(6) \qquad (7p_2 - p_1^2)[X] \equiv 0 \pmod{45}.$$

The two congruences (5) and (6) are not independent of each other; (5) results if one multiplies (6) by -7. For $\dim X = 12$, the integrality of $\hat{A}(X)$ and $L(X)$ respectively means

$$(7) \qquad (16p_3 - 44p_2p_1 + 31p_1^3)[X] \equiv 0 \pmod{945},$$

$$(8) \qquad (62p_3 - 13p_2p_1 + 2p_1^3)[X] \equiv \pmod{945}.$$

In this case, neither of the two congruences is a formal consequence of the other, since one can derive from (7) and (8) that

$$(9) \qquad (p_1p_2)[X] \equiv 0 \pmod{3}.$$

(8) is a formal consequence of (7) and (9), and (7) of (8) and (9). The congruence (9) can also be obtained by the use of Steenrod's reduced powers. In fact, by [15, Theorem 2.1],

$$p_1^3 \equiv -p_1(7p_2 - p_1^2) \pmod{3}.$$

Assume now that X is a compact connected oriented differentiable manifold of dimension $2q$, whose real Pontrjagin classes p_j vanish for $j \neq 0, \dim X$. Taking into account that $\hat{A}(X)$ is integral exc 2, we get

(10) $\qquad d^q[X]/q!$ *is integral* exc 2 *for all* $d \in H^2(X, \mathbf{Z})$

and also, by 25.5,

(11) $\qquad \mathrm{ch}(\eta)[X]$ *is integral* exc 2 *for every* $\boldsymbol{U}(k)$*-bundle over* X.

Let c_j be the Chern classes of η. We infer from the definition of the Chern character (9.1) that for $q \neq 0$, the $2q$-dimensional component $\mathrm{ch}(\eta)_q$ of $\mathrm{ch}\,\eta$ is of the form

$$(12) \qquad q!\,\mathrm{ch}(\eta)_q = (-1)^{q+1} q \cdot c_q + P(c_1, \cdots, c_{q-1}),$$

where P is a polynomial in $q-1$ indeterminates with integral coefficients. Therefore (11) and (12) prove in particular the following:

25.8. THEOREM. *Let ξ be a $\boldsymbol{U}(k)$-bundle over $\boldsymbol{S}_{2q}$, and let c_q be its q-th Chern class. Then $c_q[\boldsymbol{S}_{2q}]/(q-1)!$ is an integer* exc 2.

The theorem is non trivial only for $k \geqq q$. For $q = k$, it implies that the spheres $\boldsymbol{S}_{2q}$ are not almost complex for $q \geqq 4$. (See also [18, § 2.1].) This was proved by Borel-Serre by showing that $c_q[\boldsymbol{S}_{2q}]$ is divisible by every prime p less than q and not dividing q, see [6, Propositions 12.4 and 15.1].

25.9. COROLLARY. *Let η be a principal $\boldsymbol{O}(k)$-bundle ($\boldsymbol{Sp}(k)$-bundle) over the sphere $\boldsymbol{S}_{4q}$. Let p_q (respectively e_q) be the q-th Pontrjagin class (q-th symplectic Pontrjagin class) of η. Then*

$$p_q[\boldsymbol{S}_{4q}]/(2q-1)! \text{ or } e_q[\boldsymbol{S}_{4q}]/(2q-1)! \text{ respectively}$$

is an integer exc 2.

For the proof, it is enough to observe that p_q (respectively e_q) is by definition up to sign the Chern class c_{2q} of the complex extension η' of η, with respect to the inclusion $\boldsymbol{O}(k) \subset \boldsymbol{U}(k)$ (respectively $\boldsymbol{Sp}(k) \subset \boldsymbol{U}(2k)$), and then to apply Theorem 25.8 to η'.

26. Applications to homotopy groups of Lie groups. In this paragraph, C_2 will be the class of finite commutative 2-groups.

26.1. The boundary homomorphism in the homotopy sequence of a bundle ξ will be denoted by ∂_ξ. We recall that there is a commutative diagram

$$\begin{tikzcd} \pi_i(B_\xi) \arrow[r, leftrightarrow] \arrow[d, "\alpha"] & \pi_i(E_\xi \bmod F) \arrow[r, "\partial_\xi"] \arrow[d, "\alpha"] & \pi_{i-1}(F) \arrow[d, "\alpha"] \\ H_i(B_\xi, \boldsymbol{Z}) & H_i(E_\xi \bmod F, \boldsymbol{Z}) \arrow[l] \arrow[r, "\partial_*"] & H_{i-1}(F, \boldsymbol{Z}), \end{tikzcd} \tag{1}$$

where F is some fibre, ∂_* the boundary homomorphism of the relative homology sequence and α the Hurewicz homomorphism. Using the bottom line of (1) to define transgression in homology and the corresponding maps

$$H^i(B_\xi, \boldsymbol{Z}) \longrightarrow H^i(E_\xi \bmod F, \boldsymbol{Z}) \xleftarrow{\partial^*} H^{i-1}(F, \boldsymbol{Z})$$

to define the transgression τ_ξ in cohomology, we obtain readily the:

PROPOSITION. *Let $x \in \pi_i(B_\xi)$ and let $y \in H^{i-1}(F_\xi, \boldsymbol{Z})$ be transgressive. Then for any image $\tau_\xi(y) \in H^i(B_\xi, \boldsymbol{Z})$ of y by transgression, we have*

$$KI(\tau_\xi(y), \alpha(x)) = KI(y, \alpha\partial_\xi x),$$

where KI (for Kronecker index) denotes the standard pairing of homology and cohomology.

26.2. ι_n will denote a generator of $\pi_n(\boldsymbol{S}_n)$ or its image in $H_n(\boldsymbol{S}_n, \boldsymbol{Z})$, and $\iota_n{}^*$ the dual generator of $H^n(\boldsymbol{S}_n, \boldsymbol{Z})$. We recall [26, § 18.5] that if we associate to a principal G-bundle ξ over $\boldsymbol{S}_n$ the element $\partial_\xi(\iota_n) \in \pi_{n-1}(G)$, we define a 1-1 correspondence between the set of equivalence classes of principal G-bundles over $\boldsymbol{S}_n$ and $\pi_{n-1}(G)$. Also, since for any finite dimension, we may take a differentiable manifold as classifying space for G, each equivalence class may be represented by a differentiable bundle, and we shall assume our bundles to be differentiable whenever convenient. Clearly, if $\lambda\colon G \to G'$ is a homomorphism and if the G-bundle ξ is represented by α, then its λ-extension is represented by $\lambda_0(\alpha)$, where $\lambda_0\colon \pi_{n-1}(G) \to \pi_{n-1}(G')$ is induced by λ.

We shall be interested in the cases $n = 2q$, $G = \boldsymbol{U}(m)$ $(m \geqq q)$, $n = 4q$, $G = \boldsymbol{Sp}(r)$, $(r \geqq q)$, $n = 4q$, $G = \boldsymbol{SO}(s)$ $(s \geqq 2q+1)$, and shall denote by c^*_k or $c^*_k(\xi)$ (respectively e^*_k or $e^*_k(\xi)$, respectively p^*_k or $p^*_k(\xi)$) the value of the k-th Chern (respectively symplectic Pontrjagin, respectively Pontrjagin) class on ι_n, where $n = 2k$ (respectively $n = 4k$, respectively $n = 4k$). It follows directly from the definition of the characteristic classes by means of classifying spaces that $\xi \to c^*_k(\xi)$ (respectively $\xi \to e^*_k(\xi)$, respectively $\xi \to p^*_k(\xi)$) is a homomorphism of the $(n-1)$-th homotopy group $\pi_{n-1}(G)$ of the structural group into $\boldsymbol{Z}$; hence this homomorphism depends only on $\pi_{n-1}(G)$ modulo torsion. Finally, we recall that the maps

$$\pi_{2q-1}(\boldsymbol{U}(r)) \to \pi_{2q-1}(\boldsymbol{U}(s)), \pi_{4q-1}(\boldsymbol{Sp}(r)) \to \pi_{4q-1}(\boldsymbol{Sp}(s)) \quad (s \geqq r \geqq q)$$
$$\pi_{4q-1}(\boldsymbol{SO}(r)) \to \pi_{4q-1}(\boldsymbol{SO}(s)) \quad (s \geqq r \geqq 4q+1)$$

induced by the standard inclusions are isomorphisms [26, § 22.8, 25.2, 25.5] and that

$$\pi_{4q-1}(\boldsymbol{SO}(2r+1)) \to \pi_{4q-1}(\boldsymbol{SO}(2s+1)), \qquad (s \geqq r \geqq q),$$

is an isomorphism mod C_2; this last fact follows from the homotopy sequence of the fibering $\boldsymbol{SO}(2r+1)/\boldsymbol{SO}(2r-1) = \boldsymbol{W}_{4r-1}$, where $\boldsymbol{W}_{4r-1}$ is the manifold of unit tangent vectors to $\boldsymbol{S}_{2r}$, and from the existence of a map $\boldsymbol{S}_{4r-1} \to \boldsymbol{W}_{4r-1}$ which induces a C_2-isomorphism of $\pi_i(\boldsymbol{S}_{4r-1})$ onto $\pi_i(\boldsymbol{W}_{4r-1})$ for all $i \geqq 0$ (see [25], Chapitre IV, Prop. 2).

26.3. LEMMA. (a) *Let ξ be a principal $\boldsymbol{U}(q)$-bundle over $\boldsymbol{S}_{2q}$, and let η be the associated bundle with fibre $\boldsymbol{S}_{2q-1} = \boldsymbol{U}(q)/\boldsymbol{U}(q-1)$. Then*

$$\partial_\eta(\iota_{2q}) = \pm\, c^*_q(\xi) \cdot \iota_{2q-1}$$

(b) *Let ξ be a principal $\boldsymbol{Sp}(q)$-bundle over S_{4q}, and η be the associated bundle with fibre $S_{4q-1}=\boldsymbol{Sp}(q)/\boldsymbol{Sp}(q-1)$. Then $\partial_\eta \iota_{4q}=\pm e^*_q(\xi)\iota_{4q-1}$.*

The assertion (a) follows from the fact that $c_q(\xi)$ is the image by transgression of $\pm\iota_{2q-1}$ in η (see § 29) and from 26.1.

By definition, $e_q(\xi)=(-1)^q c_{2q}(\xi')$, where ξ' is the λ-extension of ξ under the inclusion $\lambda\colon \boldsymbol{Sp}(q)\to \boldsymbol{U}(2q)$. It is immediately seen that the pair inclusion $(\boldsymbol{Sp}(q-1),\boldsymbol{Sp}(q))\to(\boldsymbol{U}(2q-1),\boldsymbol{U}(2q))$ induces a homeomorphism of $\boldsymbol{Sp}(q)/\boldsymbol{Sp}(q-1)$ onto $\boldsymbol{U}(2q)/\boldsymbol{U}(2q-1)$. As a consequence, the bundle (ξ',S_{4q-1}) associated to ξ' is the λ-extension of η, and then (b) is implied by (a).

26.4. The result quoted at the end of 26.2 implies in particular that $\pi_{4q-1}(\boldsymbol{W}_{4q-1})$ is the direct sum of $\boldsymbol{Z}$ and of a finite 2-group, and that there exists an integer $2^{a(q)}$ such that the image of the Hurewicz homomorphism

$$\alpha\colon \pi_{4q-1}(\boldsymbol{W}_{4q-1})\to H_{4q-1}(\boldsymbol{W}_{4q-1},\boldsymbol{Z})$$

is generated by $2^{a(q)}\cdot j_q$, where j_q is a generator of $H_{4q-1}(\mathbf{W}_{4q-1},\boldsymbol{Z})$.

Lemma. *Let ξ be a principal $\boldsymbol{SO}(2q+1)$-bundle over S_{4q}, η be the associated bundle with fibre $\boldsymbol{W}_{4q-1}=\boldsymbol{SO}(2q+1)/\boldsymbol{SO}(2q-1)$, and let γ_q be a generator of $\pi_{4q-1}(\boldsymbol{W}_{4q-1})$*mod *2-torsion. Then we have in the previous notation*

$$\partial_\eta\iota_{4q}=\pm 2^{-a(q)-1}p^*_q(\xi)\gamma_q \text{ modulo } 2\text{-}torsion.$$

Modulo 2-torsion, we have $\partial_\eta\iota_{4q}=c\cdot\gamma_q$, for some integer c, and therefore

$$\alpha\partial_\eta\iota_{4q}=2^{a(q)}\cdot c\cdot j_q.$$

By § 30, $p_q(\xi)$ is the image by transgression in η of $\pm 2j_q^*$, where j_q^* is the generator of $H^{4q-1}(\boldsymbol{W}_{4q-1},\boldsymbol{Z})$ dual to j_q. Hence we have by 26.1

$$\pm p^*_q(\xi)=KI(2j_q^*,\ \alpha\partial_\eta\iota_{4q})=2^{a(q)+1}\cdot c$$

which proves the lemma.

26.5. Theorem. There exists:

(a) *over S_{2q} a $\boldsymbol{U}(m)$-bundle with $c^*_q=(q-1)!$ for $m\geqq q$.*

(a*) *over S_{4q} a $\boldsymbol{SO}(n)$-bundle with $p^*_q=(2q-1)!\cdot 2$ for $n\geqq 4q$ and a $\boldsymbol{Sp}(m)$-bundle with $e^*_q=(2q-1)!\cdot 2$ for $m\geqq q$.*

(b) *over S_{4q}, q even, a $\boldsymbol{SO}(n)$-bundle with $p^*_q=(2q-1)!$ for $n\geqq 4q+1$ (for $n\geqq 8$ if $q=2$).*

(c) *over* S_{4q}, q *odd, a* $\boldsymbol{Sp}(m)$*-bundle with* $e^*_q = (2q-1)!$ *for* $m \geqq q$.

(d) *over* S_{4q} *a* $\boldsymbol{SO}(n)$*-bundle with* p^*_q *equal, up to a power of 2, to the greatest odd factor of* $(2q-1)!$ *for* $n \geqq 2q+1$.

By 26.2 and the end remark in 9.7, it is enough to prove (a), (b), (c) for one particular value of m or n; (d) follows from (a*). The case $q=2$ in (b) will be dealt with in 26.6.

Let η be the principal $\boldsymbol{SO}(2q)$-bundle of the tangential bundle to S_{2q}, and let $\lambda\colon \boldsymbol{Spin}(2q) \to \boldsymbol{SO}(2q)$ be the covering map. Since $w_2(\eta)=0$, the bundle η may be λ-restricted to a principal $\boldsymbol{Spin}(2q)$-bundle. In fact, $\rho(\lambda)\colon B_{\boldsymbol{Spin}(n)} \to B_{\boldsymbol{SO}(n)}$ is (for any $n \geqq 2$) a fibre map with fibre B_{Z_2} (see [2] § 22 or [6] § 1), i.e. an Eilenberg-MacLane space $K(\boldsymbol{Z}_2, 1)$; its spectral sequence shows readily that the obstruction to a cross section is the universal second Stiefel-Whitney class w_2; then, by a standard argument, every map $\sigma\colon B \to B_{\boldsymbol{SO}(n)}$ with $\sigma^*(w_2)=0$ can be factorized through $\rho(\lambda)$, and this shows in our case the existence of a λ-restriction η' of η.

Let x_i, $(1 \leqq i \leqq q)$, be the standard basis of the usual maximal torus $\boldsymbol{T}$ of $\boldsymbol{SO}(2q)$, and let $\boldsymbol{T}'$ be the inverse image of $\boldsymbol{T}$ in $\boldsymbol{Spin}(2q)$; it is connected (see 10.1) and is a maximal torus of $\boldsymbol{Spin}(2q)$; we shall also denote by x_i the image of x_i in $H^1(\boldsymbol{T}', \boldsymbol{Z})$ under the covering map; these generate a subgroup of index 2 of $H^1(\boldsymbol{T}', \boldsymbol{Z})$. Let $\beta\colon \boldsymbol{Spin}(2q) \to \boldsymbol{U}(2^{q-1})$ be one of the half-spinor representations, say the one with the highest weight $\frac{1}{2}(x_1 + \cdots + x_q)$, and let θ be the β-extension of η'). We want to prove

$$c_q(\theta) = (-1)^{q-1}(q-1)! \cdot \iota_{2q} \tag{2}$$

which,[4] in view of our initial remark, will prove (a). Let ω_j $(1 \leqq j \leqq 2^{q-1})$, be the weights of β. It is known that these are just the linear forms

$$\tfrac{1}{2}(\epsilon_1 x_1 + \cdots + \epsilon_q x_q), \quad (\epsilon_i = \pm 1, (i=1,\cdots,q), \textstyle\prod \epsilon_i = 1)$$

(in fact, these are all transforms under the Weyl group $W(\boldsymbol{SO}(2q))$ of the highest weight, hence they must be weights; moreover, since there are 2^{q-1} of them, they represent all weights). Let ρ be the projection of $E_{\eta'}/T'$ onto S_{2q}. By (9.5), we have $\rho^*(W_{2q}(\eta)) = x_1 \cdots x_q$, and hence

$$x_1 \cdots x_q = 2 \cdot \rho^*(\iota_{2q}). \tag{3}$$

By (10.3), $\rho^*(c_q(\theta))$ is the q-th elementary symmetric function in the ω_j. Since the lower symmetric functions are zero here (because $H^i(S_{2q}, \boldsymbol{Z}) = 0$

[4] The other half-spinor representation yields a bundle whose q-th Chern class is $-c_q(\theta)$.

for $0 < i < 2q$), we get

$$(4) \qquad (-1)^{q-1}q\cdot\rho^*(c_q(\theta)) = \omega_1{}^q + \cdots + \omega_s{}^q, \qquad (s = 2^{q-1}).$$

Let $\omega_j = \frac{1}{2}(\epsilon_1 x_1 + \cdots + \epsilon_q x_q)$ be one particular weight. We have

$$\omega_j{}^q = q!\cdot 2^{-q}\cdot x_1\cdots x_q + b_j,$$

where b_j is a sum of monomials in the x_i's, none of which contains all variables x_i, and therefore

$$\sum \omega_j{}^q = q!\cdot 2^{-1}\cdot x_1\cdots x_q + \sum b_j$$

or, taking (3) into account,

$$\sum \omega_j{}^q = q!\cdot\rho^*(\iota_{2q}) + \sum b_j$$

so that (2) will follow from (4) if we show that

$$(5) \qquad \sum b_j = 0.$$

$W(\boldsymbol{SO}(2q))$ is the group of permutations of the x_i combined with an even number of changes of signs. Thus, the ring I_W of invariants of $W(\boldsymbol{SO}(2q))$ is generated by $x_1\cdots x_q$ and by the symmetric functions in the $x_i{}^2$. The Weyl group permutes the ω_j, and therefore $\sum b_j \in I_W$; since no monomial in this sum contains all variables x_i's, b_j must then be a symmetric function in the $x_i{}^2$; but, by (9.3), it is then the image under ρ^* of a polynomial in the Pontrjagin classes of η. Since the Pontrjagin classes of $\boldsymbol{S}_{2q}$ are all zero, this proves (5).

Let now $q = 2s$ be even; let ξ be the $\boldsymbol{U}(2s)$-bundle over $\boldsymbol{S}_{4s}$ with Chern class $(2s-1)!$, and ξ^* be its extension under the contragredient representation (10.6). We have $c_{2s}(\xi) = c_{2s}(\xi^*)$, hence

$$c_{2s}(\xi \oplus \xi^*) = (2s-1)!\cdot 2\cdot\iota_{4s},$$

but in $\boldsymbol{U}(4s)$, the matrices of the form $A \dotplus \bar{A}$ ($A \in \boldsymbol{U}(2s)$) form a subgroup conjugate to a subgroup of $\boldsymbol{Sp}(2s)$ or of $\boldsymbol{SO}(4s)$, and $\xi \oplus \xi^*$ can be considered as the complexification of a $\boldsymbol{Sp}(2s)$- or of a $\boldsymbol{SO}(4s)$-bundle. This proves (a*).

It is known that the image group of a half-spinor representation of $\boldsymbol{SO}(4q)$ is conjugate to a subgroup of $\boldsymbol{SO}(2^{2q-1})$ (respectively $\boldsymbol{Sp}(2^{2q-2})$), if q is even (respectively odd). (See E. Cartan, Jour. Math. Pur. Appl. 10 (1914), 149-186, § XV, p. 173, or A. I. Malcev, Isv. Ak. Nauk. SSSR Ser. Math. 8 (1944), 143-174, A. M. S. Translation 33, pp. 29-30.) This implies that θ is the complexification of a $\boldsymbol{SO}(2^{2q-1})$- (respectively $\boldsymbol{Sp}(2^{2q-2})$-) bundle, for q even (respectively odd), and (b) and (c) follow from (2).

26.6. *Remark.* The image group of $\boldsymbol{Spin}(8)$ under a half-spinor representation is conjugate to $\boldsymbol{SO}(8)$, as is well known and follows also from the result just quoted. The standard representation of $\boldsymbol{SO}(8)$ and the two half-spinor representations provide three homomorphisms of $\boldsymbol{Spin}(8)$ onto $\boldsymbol{SO}(8)$ which are, up to equivalence, all the representations of degree 8 of $\boldsymbol{Spin}(8)$. They may be distinguished by the element or order 2 of the center of $\boldsymbol{Spin}(8)$, (isomorphic to $\boldsymbol{Z}_2+\boldsymbol{Z}_2$), which they map onto the identity. They may be obtained from one another by performing on $\boldsymbol{Spin}(8)$ the automorphisms of the triality principle, (which are transitive on the elements of the center of $\boldsymbol{Spin}(8)$ different from the identity).

The last step of the proof of 26.5 shows therefore that θ is a $\boldsymbol{SO}(8)$-bundle over $\boldsymbol{S}_8$ with $p^*{}_2=-6$, which ends the proof of (b). On the other hand, the projective lines on the Cayley plane $\boldsymbol{W}$ are homeomorphic to $\boldsymbol{S}_8$ and a generator u of $H^8(\boldsymbol{W},\boldsymbol{Z})$ restricts on them to a fundamental cocycle; therefore 9.7 and 19.4 show that the normal bundle θ' to a projective line in $\boldsymbol{W}$ has also $p^*{}_2=-6$. In fact, it can be shown directly that θ and θ' are isomorphic; we sketch the proof, using 19.1 and some information on $\boldsymbol{W}$ to be found for instance in [1]: Let $\boldsymbol{U}$ be a subgroup of $\boldsymbol{F}_4$ isomorphic to $\boldsymbol{Spin}(9)$, $\boldsymbol{V}$ a subgroup of $\boldsymbol{U}$ isomorphic to $\boldsymbol{Spin}(8)$, and P the point of $\boldsymbol{W}$ fixed under $\boldsymbol{U}$. Then $\boldsymbol{V}$ leaves exactly two other points Q, R fixed, and the projective line M joining Q, R is operated upon transitively by $\boldsymbol{U}$. Thus the fibering $\xi=(\boldsymbol{U},\boldsymbol{U}/\boldsymbol{V},\boldsymbol{V})$ may be identified with $(\boldsymbol{Spin}(9),\ \boldsymbol{S}_8,\ \boldsymbol{Spin}(8))$. The natural representation of $\boldsymbol{V}$ into the tangent space $\boldsymbol{W}_Q$ of $\boldsymbol{W}$ at Q decomposes into the representations ρ_1, ρ_2 into M_Q and into the subspace N_Q of $\boldsymbol{W}_Q$ orthogonal to M_Q. Thus the tangent (respectively normal) bundle to M is the ρ_1- (respectively ρ_2-) extension of ξ. The representation of $\boldsymbol{V}$ in $\boldsymbol{W}_Q$ is faithful, because its kernel belongs to the center of $\boldsymbol{F}_4$, which is reduced to $\{e\}$. Hence (see beginning of this section) ρ_1 and ρ_2 are not equivalent, the normal bundle to M and the bundle θ of 26.5 arise from the tangent bundle to $\boldsymbol{S}_8$ by the same construction.

26.7. THEOREM. *The fibrations*

$$\boldsymbol{U}(q)/\boldsymbol{U}(q-1)=\boldsymbol{S}_{2q-1},\qquad \boldsymbol{Sp}(q)/\boldsymbol{Sp}(q-1)=\boldsymbol{S}_{4q-1},$$

$$\boldsymbol{SO}(2q+1)/\boldsymbol{SO}(2q-1)=\boldsymbol{W}_{4q-1},\qquad \boldsymbol{G}_2/\boldsymbol{Sp}(1)=\boldsymbol{W}_{11}$$

give rise to the following sequences, which are exact modulo the class C_2 of finite commutative 2-groups:

(a) $\quad 0\to\boldsymbol{Z}_{(q-1)!}\to\pi_{2q-2}(\boldsymbol{U}(q-1))\to\pi_{2q-2}(\boldsymbol{U}(q))\to 0 \qquad (q\geqq 2)$

(b) $0 \to \boldsymbol{Z}_{(2q-1)!} \to \pi_{4q-2}(\boldsymbol{Sp}(q-1)) \to \pi_{4q-2}(\boldsymbol{Sp}(q)) \to 0$ $(q \geqq 2)$

(c) $0 \to \boldsymbol{Z}_{(2q-1)!} \to \pi_{4q-2}(\boldsymbol{SO}(2q-1)) \to \pi_{4q-2}(\boldsymbol{SO}(2q+1)) \to 0$ $(q \geqq 2)$

(d) $0 \to \boldsymbol{Z}_{k15} \to \pi_{10}(\boldsymbol{S}_3) \to \pi_{10}(\boldsymbol{G}_2) \to 0$, *for some* $k \geqq 1$.[5]

(a) Let $\alpha \in \pi_{2q-1}(\boldsymbol{U}(q))$. Let ξ be a principal $\boldsymbol{U}(q)$-bundle over $\boldsymbol{S}_{2q}$ representing α, and η be the associated bundle with fibre $\boldsymbol{S}_{2q-1}$. Then $E_\eta = E_\xi/\boldsymbol{U}(q-1)$ and the restriction of the natural map $E_\xi \to E_\eta$ to a fibre is the projection map in the fibering $(\boldsymbol{U}(q), \boldsymbol{S}_{2q-1}, \boldsymbol{U}(q-1))$ hence we get a commutative diagram

$$\begin{array}{ccc} \pi_{2q}(\boldsymbol{S}_{2q}) & \xrightarrow{\partial_\eta} & \pi_{2q-1}(\boldsymbol{S}_{2q-1}) \\ \updownarrow & & \uparrow \psi \\ \pi_{2q}(\boldsymbol{S}_{2q}) & \xrightarrow{\partial_\xi} & \pi_{2q-1}(\boldsymbol{U}(q)), \end{array}$$

where ψ is part of the homotopy sequence of $(\boldsymbol{U}(q), \boldsymbol{S}_{2q-1}, \boldsymbol{U}(q-1))$. By definition, $\alpha = \partial_\xi(\iota_{2q})$, hence we have by 26.3a.

$$\psi(\alpha) = \pm c^*{}_q(\xi)\iota_{2q-1}$$

which is divisible by the greatest odd factor of $(q-1)!$ in virtue of 25.8. Since α is arbitrary, this shows that $\psi(\pi_{2q-1}(\boldsymbol{U}(q))$ is contained in the subgroup generated by $b(q-1)\cdot\iota_{2q-1}$, where $b(q-1)$ is the greatest odd factor of $(q-1)!$; on the other hand, the same argument together with (26.5), shows that $\psi(\pi_{2q-1}(\boldsymbol{U}(q)))$ contains $(q-1)!\cdot\iota_{2q-1}$, and the mod C_2 exactness of (a) follows.

The proofs for (b) and (c) are quite analogous, the sole difference being that one has to invoke 26.3b and 26.4 instead of 26.3a.

For the fibration $\boldsymbol{G}_2/\boldsymbol{Sp}(1) = \boldsymbol{W}_{11}$, we refer to [4, § 17]. Let $\alpha \in \pi_{11}(\boldsymbol{G}_2)$, let ξ be a principal $\boldsymbol{G}_2$-bundle representing α, and let η be the associated bundle with fibre $\boldsymbol{W}_{11}$. We have the commutative diagram

$$(6) \qquad \begin{array}{ccc} \pi_{12}(\boldsymbol{S}_{12}) & \xrightarrow{\partial_\eta} & \pi_{11}(\boldsymbol{W}_{11}) \\ \updownarrow & & \uparrow \psi \\ \pi_{12}(\boldsymbol{S}_{12}) & \xrightarrow{\partial_\xi} & \pi_{11}(\boldsymbol{G}_2). \end{array}$$

Now $\boldsymbol{G}_2$ is embedded in $\boldsymbol{SO}(7)$ and its action on $\boldsymbol{W}_{11}$ extends to that of $\boldsymbol{SO}(7)$; in other words, $\boldsymbol{G}_2$, as a subgroup of $\boldsymbol{SO}(7)$, acts transitively on $\boldsymbol{W}_{11} = \boldsymbol{SO}(7)/\boldsymbol{SO}(5)$ and $\boldsymbol{G}_2 \cap \boldsymbol{SO}(5) = \boldsymbol{Sp}(1)$. This means that if we

[5] It will be shown later that $k = 1$.

extend the structural group of η to $\boldsymbol{SO}(7)$, we get the associated bundle to the extension ξ' of ξ. Therefore we have by 26.4:

$$\partial\eta(\iota_{12}) = \pm 2^{-a(3)-1} p^*_3(\xi')\gamma_3 \bmod 2\text{-torsion}$$

and (6) gives then: $\psi(\alpha) = \pm p^*_3(\xi')\cdot\gamma_3$, up to a power of two. Since (25.9) the number $p^*_3(\xi')$ is divisible by 15, and since this argument is valid for any $\alpha \in \pi_{11}(\boldsymbol{G}_2)$, the mod C_2 exactness of (d) is established.

26.8. PROPOSITION. *If we have*

$$(7) \qquad \pi_9(\boldsymbol{SO}(7)) \equiv 0, \qquad \pi_{10}(\boldsymbol{U}(5)) \equiv \boldsymbol{Z}_{15} \bmod C_2,$$

then the following congruences mod C_2 *are valid:* $\pi_{10}(\boldsymbol{G}_2) \equiv 0$, $\pi_{10}(\boldsymbol{SO}(5)) \equiv \boldsymbol{Z}_{15}$, $\pi_{10}(\boldsymbol{SO}(n)) \equiv 0$ $(n \geqq 7, n \neq 8)$, $\pi_{10}(\boldsymbol{Sp}(n)) \equiv 0$ $(n \geqq 3)$, $\pi_{10}(\boldsymbol{U}(n)) \equiv 0$ $(n \geqq 6)$.

In this proof, all congruences are mod C_2. We use the following results:

$$(8) \qquad \pi_{n+1}(\boldsymbol{S}_n) \equiv \pi_{n+2}(\boldsymbol{S}_n) \equiv 0 \quad (n \geqq 3), \qquad \pi_{n+3}(\boldsymbol{S}_n) \equiv \boldsymbol{Z}_3 \quad (n \geqq 5),$$

$$(9) \qquad \pi_{10}(\boldsymbol{S}_3) \equiv \boldsymbol{Z}_{15}, \qquad \pi_9(\boldsymbol{S}_3) \equiv \boldsymbol{Z}_3.$$

(For the last equality of (8), see J-P. Serre, Comm. Math. Helv. 27 (1953), 198-232, for the other ones, see [25]; as to (7), see 26.9 and 26.10 below.)

The first equality in (9) shows that in 26.7d, we have $k=1$ and $\pi_{10}(\boldsymbol{G}_2) \equiv 0$. The fibering $\boldsymbol{G}_2/\boldsymbol{Sp}(1) = \boldsymbol{W}_{11}$, discussed in [4, § 17], together with (9) and the congruence $\pi_i(\boldsymbol{W}_{11}) \equiv \pi_i(\boldsymbol{S}_{11})$ shows that $\pi_9(\boldsymbol{G}_2) \equiv \boldsymbol{Z}_3$. Applying this and (7) to the exact homotopy sequence of the fibering $\boldsymbol{Spin}(7)/\boldsymbol{G}_2 = \boldsymbol{S}_7$ (see [1]), we get the mod C_2 exact sequence

$$0 \to \pi_{10}(\boldsymbol{SO}(7)) \to \boldsymbol{Z}_3 \to \boldsymbol{Z}_3 \to 0;$$

hence $\pi_{10}(\boldsymbol{SO}(7)) \equiv 0$. The mod C_2 exact sequence 26.7c yields then, for $q=3$, that $\pi_{10}(\boldsymbol{SO}(5)) \equiv \boldsymbol{Z}_{15}$. Since, as is well known, the universal covering $\boldsymbol{Spin}(5)$ of $\boldsymbol{SO}(5)$ is isomorphic to $\boldsymbol{Sp}(2)$, we deduce from 26.7b that $\pi_{10}(\boldsymbol{Sp}(3)) \equiv 0$, and hence also $\pi_{10}(\boldsymbol{Sp}(n)) \equiv 0$ for $n \geqq 3$.

Since $\boldsymbol{SO}(9)/\boldsymbol{SO}(7) = \boldsymbol{W}_{15}$ has, mod C_2, the homotopy groups of $\boldsymbol{S}_{15}$, we have $\pi_{10}(\boldsymbol{SO}(9)) \equiv \pi_{10}(\boldsymbol{SO}(7)) \equiv 0$ and then $\pi_{10}(\boldsymbol{SO}(n)) \equiv 0$ $(n \geqq 9)$ follows from (8), the finiteness of $\pi_{10}(\boldsymbol{SO}(11))$ (see [25]) and the homotopy sequence of $\boldsymbol{SO}(n)/\boldsymbol{SO}(n-1) = \boldsymbol{S}_{n-1}$.

Finally, (7) and 26.7a give $\pi_{10}(\boldsymbol{U}(6)) \equiv 0$, and therefore $\pi_{10}(\boldsymbol{U}(n)) \equiv 0$ for $n \geqq 6$.

26.9. The preceding results (found in Spring 1957) contradict several

of those of [30]. Since then, Toda has made new computations whose outcome (yet unpublished) agrees with the above. They have also been confirmed by Bott (Proc. Nat. Ac. Sci. USA 43 (1957), pp. 933-935) who in particular determines all stable homotopy groups of the classical groups.

26.10. Bott has also shown (to be published) that the sequence 26.7(a) is exact also for the 2-primary components (since $\pi_{2q-2}(\boldsymbol{U}(q))=0$, by Bott, loc. cit., 26.9, this gives $\pi_{2q-2}(\boldsymbol{U}(q-1))=\boldsymbol{Z}_{(q-1)!}$). This implies (see 26.3 and the proof of 26.7) the following generalization of 25.8, 25.9:

THEOREM (Bott). *Let ξ be a $\boldsymbol{U}(k)$-bundle over $\boldsymbol{S}_{2q}$. Then $c^*_q(\xi)$ is divisible by $(q-1)!$. Let η be a $\boldsymbol{SO}(k)$- (respectively $\boldsymbol{Sp}(k)$-), bundle over over $\boldsymbol{S}_{4q}$. Then $p^*_q(\eta)$ (respectively $e^*_q(\eta)$), is divisible by $(2q-1)!$.*

Using this theorem, Kervaire has proved more generally that $p^*_q(\eta)$ (respectively $e^*_q(\eta)$) is divisible by $(2q-1)!\cdot 2$ if q is odd (respectively even) (Amer. Jour. Math., vol. 80 (1958), pp. 632-638).

The stable homotopy groups $\pi_{2q-1}(\boldsymbol{U}(k))$, $(k\geqq q)$, and $\pi_{4q-1}(\boldsymbol{SO}(k))$ $(k\geqq 4q+1)$ are infinite cyclic according to Bott (loc. cit. in 26.9). The generator of the first group has the Chern number $c^*_q=\pm(q-1)!$, the generator of the second group has Pontrjagin number p^*_q equal to $\pm(2q-1)!$ if q is even and $\pm(2q-1)!\cdot 2$ if q is odd; similarly for the symplectic groups (with odd and even interchanged). This follows from the preceding theorem, the result of Kervaire and 26.5. The "spinor-method" in 26.5 gives an explicit construction for these generators.

The above theorem would follow by the same argument as 25.8, 25.9 if one could prove that the virtual Todd genus with respect to an *integral* class is an integer. In this respect, compare the conjectures in 25.6. The last one would contain Kervaire's result for the orthogonal groups.

Finally, we remark that the proof of 25.8, 25.9 also applies if the sphere is replaced by a compact connected oriented manifold X whose real Pontrjagin classes p_j vanish for $4j\neq 0$, $\dim X$, and if ξ (respectively η) is a $\boldsymbol{U}(k)$-bundle (respectively $\boldsymbol{O}(k)$- or $\boldsymbol{Sp}(k)$-bundle) whose real Chern (respectively Pontrjagin or symplectic Pontrjagin) classes vanish in all positive dimensions less than $\dim X$.

26.11. Milnor and Kervaire, independently, have deduced from the result of Bott quoted in 26.10 that $\boldsymbol{S}_n$, endowed with its usual differentiable structure, is not parallelizable if $n\neq 1, 3, 7$. An easy argument similar to 26.3 shows that if $\boldsymbol{S}_{2n-1}$ is parallelizable, that is if the fibering $\boldsymbol{SO}(2n)/\boldsymbol{SO}(2n-1)$ $=\boldsymbol{S}_{2n-1}$ has a cross section, then there exists a $\boldsymbol{SO}(2n)$-bundle η over $\boldsymbol{S}_{2n}$.

whose Euler-Poincaré class W_{2n} is equal to $1 \cdot \iota_{2n}$. Therefore the theorem of Milnor-Kervaire is a consequence of the

THEOREM (Milnor). *Let ξ be a $\boldsymbol{SO}(2q)$-bundle over S_{2q}, where $q \neq 1, 2, 4$. Then $W_{2q}(\xi)$ is divisible by 2.*

We want to give here a proof for this, different from Milnor's but also using 26.10.

Let η be a $\boldsymbol{SO}(2q)$-bundle whose second Stiefel-Whitney class w_2 vanishes. Then (see beginning of the proof of 26.5), η has a λ-restriction η', where λ is the projection of $\boldsymbol{Spin}(2q)$ onto $\boldsymbol{SO}(2q)$. We denote again by θ the extension of η' by means of the half-spinor representation β. It is a $\boldsymbol{U}(2^{q-1})$-bundle.

LEMMA. *In the previous notations, we have*

(i) $c_q(\theta)/(q-1)! = W_{2q}(\eta)/2$ *if q is odd,*

(ii) $c_{2k}(\theta)/(2k-1)!$

$$= -(tg^{(2k-1)}(0)/((2k-1)!4))p_k(\eta) - W_{4k}(\eta)/2 + R_{2k}(\eta) \quad \text{if } q = 2k \geqq 2,$$

where $R_{2k}(\eta)$ is a polynomial with rational coefficients in $p_1(\eta), \cdots p_{k-1}(\eta)$, and $tg^{(2k-1)}(0)$ denotes the $(2k-1)$-th derivative of $tg\, x$ at $x = 0$.

We keep the notations of 26.5. Since ρ^* is injective, we allow ourselves to omit the symbol ρ^*. The computations of 26.5 show first that

$$\sum \omega_j^q = q! \cdot x_1 \cdots x_q/2 + q!\, r'_q(x_1^2, \cdots, x_q^2), \tag{10}$$

where r'_q has rational coefficients; this can be written

$$\sum \omega_j^q = q!\, W_{2q}(\eta)/2 + q! \cdot r_q, \tag{11}$$

r_q being a polynomial in the $p_i(\eta)$ with rational coefficients. On the other hand, $c_q(\theta)$ is the q-th elementary symmetric function in the ω_j's, hence

$$\sum \omega_j^q = (-1)^{q-1} q \cdot c_q(\theta) + q!\, s_q,$$

where s_q is a polynomial in the $c_i(\theta)$ $(i < q)$ with rational coefficients. Now, θ is extension of a $\boldsymbol{Spin}(2q)$-bundle η', hence its characteristic ring is contained in the characteristic ring of η'. Since we consider real cohomology, $\rho^*(\lambda): H^*(B_{SO(2q)}) \to H^*(B_{Spin(2q)})$ is an isomorphism, and therefore the $c_i(\theta)$ belong to the characteristic ring of η, which is generated by the $p_i(\eta)$ $(i < q)$ and by $W_{2q}(\eta)$. Thus we get

$$(-1)^{q-1}c_q(\theta)/(q-1)\,! = W_{2q}(\eta)/2 + t_q,$$

where $t_q = r_q - s_q$ is a polynomial in the $p_i(\eta)$ $(2i < q)$ with rational coefficients. It is necessarily zero if q is odd, and this proves (i). In order to prove (ii), we have to compute the coefficient d_k of $p_k(\eta)$ in t_{2k}. By the above, d_k is equal to the coefficient of $p_k(\eta)$ in r_{2k}. Let S be defined by $S(x_1) = -x_1$ and $S(x_i) = x_i$ $(i \geqq 2)$ and put $\sigma_j = S(\omega_j)$. The set $\{\sigma_j\}$ is then the set of forms

$$(\epsilon_1 x_1 + \cdots + \epsilon_{2k} x_{2k})/2, \quad \prod \epsilon_i = -1,$$

(which are the weights of the second half spinor representation), and (10) yields

$$\sum \sigma_j^{2k} = -(2k)\,!\,x_1 \cdots x_{2k}/2 + (2k)\,!\,r'_{2k}(x_1^2, \cdots, x_{2k}^2), \tag{12}$$

hence

$$\sum (\omega_j^{2k} + \sigma_j^{2k}) = (2k)\,!\,2 \cdot r_{2k}, \tag{13}$$

so that $2d_k$ is the coefficient of p_k in

$$((2k)\,!)^{-1} \sum (\omega_j^{2k} + \sigma_j^{2k}).$$

We have clearly

$$\sum_{\epsilon_i = \pm 1} \exp(\epsilon_1 x_1 + \cdots + \epsilon_{2k} x_{2k})/2 = 2^{2k} \prod_{j=1}^{j=2k} \cosh(x_j/2).$$

Let $\{D_j(p_1, \cdots, p_j)\}$ be the multiplicative sequence with $\cosh z^{\frac{1}{2}}/2$ as characteristic power series (this is well defined since $\cosh x$ is an even function in x). Then $2^{-2k+1}d_k$ is for $k \geqq 1$ the coefficient of p_k in D_k. The formula 1.4(10) of [19] yields therefore, (with $2d_0 = 1$),

$$2 \sum_{j \geqq 0} d_j(-z/4)^j = \cosh(\tfrac{1}{2}z^{\frac{1}{2}}) \cdot d(z/\cosh(\tfrac{1}{2}z^{\frac{1}{2}}))/dz,$$

$$2 \sum_{j \geqq 0} d_j(-z/4)^j = 1 - (z^{\frac{1}{2}}/4)\operatorname{tgh}(\tfrac{1}{2}z^{\frac{1}{2}}).$$

Putting $z = -4x^2$, we get then

$$\sum_{j \geqq 1} d_j x^{2j-1} = (1/4)\operatorname{tg} x,$$

and this ends the proof of (ii).

Proof of the theorem. Since the base space of ξ is $\boldsymbol{S}_{2q}$ $(q \neq 1)$, we have $w_2(\xi) = 0$, hence we may apply the lemma to ξ. For q odd, the theorem follows then from (i) and from the divisibility theorem of Bott (26.10). Let now $q = 2k$ be even. We have $tg'(0) = 1$, $tg^{(3)}(0) = 2$, and it is well known, and easily checked, that $tg^{(2k-1)}(0)$ is an integer divisible by 4 for

$k \geqq 3$. Moreover, in (ii) of the lemma we have $R_{2k} = 0$ since $B_\xi = S_{4k}$. Thus, for $q = 2k$, the theorem follows from the lemma and 26.10.

27. Multiplicative properties of the index and consequences.

27.1. *Notation.* Throughout this and the following paragraph, all cohomology groups will be taken with real coefficients and all characteristic classes which occur will be regarded as real classes unless otherwise mentioned.

$\mathfrak{D}$ denotes the class of differentiable bundles ξ, where E_ξ, B_ξ, F_ξ are compact connected oriented differentiable manifolds, the orientation of E_ξ being induced by those of B_ξ, F_ξ taken in that order, and where the fundamental group of B_ξ operates trivially on $H^*(F_\xi)$.

We recall (21.5) that if $\{K_j\}$ is a multiplicative sequence with real coefficients which is strictly multiplicative in ξ, then

$$K(E_\xi) = K(B_\xi) \cdot K(F_\xi) \qquad (\xi \in \mathfrak{D}). \tag{1}$$

We wish to prove a theorem which is a sort of converse to 21.5.

27.2. THEOREM. *Let F be a compact connected oriented differentiable manifold. If $\{K_j\}$ is a multiplicative sequence of polynomials with real coefficients, for which* (1) *holds in every bundle $\xi \in \mathfrak{D}$ such that $F_\xi = F$, then $\{K_j\}$ is strictly multiplicative in each of these bundles.*

The proof uses essentially the theorem of Thom [29, Corollaire II 30] that every real cohomology class of B_ξ is a finite linear combination of real cohomology classes representable by submanifolds. By definition, a real cohomology class is representable by a submanifold if and only if it corresponds by Poincaré duality to a real homology class containing the fundamental cycle of a compact oriented differentiable manifold differentiably imbedded in B_ξ.

The strictly multiplicative behavior of $\{K_j\}$ is obviously true if $\dim B_\xi = 0$. Let us make the induction hypothesis that it is proved for $\dim B_\xi < n$. Then we will prove it, using (1), for an n-dimensional manifold B_ξ. Let $\hat{p}_i$ be the Pontrjagin classes of the bundle along the fibres of ξ. We have to show that

$$\Big(\sum_{j=0}^{\infty} K_j(\hat{p}_1, \cdots, \hat{p}_j)\Big)^\natural = K(F_\xi) \cdot 1,$$

where $\natural : H^*(E_\xi) \to H^*(B_\xi)$ is the integration over the fibre (8.1). We can restrict the bundle ξ to every submanifold Y of B_ξ. Since integration over the fibre and restriction commute (8.3), we obtain by our induction hypothesis

that for $\dim Y < \dim B_\xi$ the restriction $(\sum_{j=0}^{\infty} K_j(\hat{p}_1,\cdots,\hat{p}_j))^\natural$ to Y equals $K(F_\xi)\cdot 1$, where 1 denotes now the unit of the cohomology ring of Y. This, together with the above mentioned theorem of Thom, implies

$$(\sum_{j=0}^{\infty} K_j(\hat{p}_1,\cdots,\hat{p}_j))^\natural = K(F_\xi)\cdot 1 + c,$$

where $c \in H^n(B_\xi)$.

We denote the Pontrjagin classes of B_ξ by p'_i and those of E_ξ by p_i. Then (compare the proof of 21.5)

$$\begin{aligned} K(E_\xi) &= (\sum_{j=0}^{\infty} K_j(p_1,\cdots,p_j))[E_\xi] \\ &= ((K(F_\xi)\cdot 1 + c)\cdot \sum_{t=0}^{\infty} K_t(p'_1,\cdots,p'_t))[B_\xi] \\ &= K(F_\xi)(\sum_{t=0}^{\infty} K_t(p'_1,\cdots,p'_t))[B_\xi] + c[B_\xi] \\ &= K(F_\xi)\cdot K(B_\xi) + c[B_\xi]. \end{aligned}$$

According to (1) we have $K(E_\xi) = K(B_\xi)K(F_\xi)$ and thus obtain $c = 0$, which completes the proof.

It was proved recently [12] for the index τ and a bundle $\xi \in \mathfrak{D}$ that

$$\tau(E_\xi) = \tau(B_\xi)\cdot\tau(F_\xi). \tag{2}$$

Since the index τ equals the genus L defined by the multiplicative sequence $\{L_j\}$, see [19, § 8], we get in virtue of the preceding theorem the following result:

27.3. THEOREM. *The sequence $\{L_j\}$ is strictly multiplicative in every $\xi \in \mathfrak{D}$.*

If $\xi \in \mathfrak{D}$ and $\natural$ is the integration over the fibre in ξ, we have therefore

$$(L_j(\hat{p}_1,\cdots,\hat{p}_j))^\natural = 0 \qquad (4j \neq \dim F_\xi),$$

$$(L_j(\hat{p}_1,\cdots,\hat{p}_j))^\natural = \tau(F_\xi)\cdot 1 \qquad (4j = \dim F_\xi).$$

27.4. *Examples.*

1) $\dim F_\xi = 2$. In this case, $\tau(F_\xi)$ vanishes. $L_j(\hat{p}_1, 0,\cdots,0)$ is a non-zero multiple of $\hat{p}_1{}^j$, see [19, § 1]. Since $\hat{p}_1 = \hat{W}_2{}^2$, where $\hat{W}_2$ is the Euler class of the bundle along the fibres, we get (in real cohomology)

$$(\hat{W}_2{}^{2j})^\natural = 0, \qquad j = 1, 2, 3, \cdots.$$

If B_ξ is of dimension $4k-2$ and hence E_ξ of dimension $4k$, then $\hat{W}_2{}^{2k}=0$.

2) $\dim F_\xi = 3$. We get for the Pontrjagin class $\hat{p}_1$ of the bundle along the fibres that $(\hat{p}_1{}^j)^\natural$ $(j=1,2,3,\cdots)$, vanishes in real cohomology.

3) $\dim F_\xi = 4$. We have $45\cdot L_2(\hat{p}_1,\hat{p}_2) = 7\hat{p}_2 - \hat{p}_1{}^2$. Thus

$$(7\hat{p}_2 - \hat{p}_1{}^2)^\natural = 0.$$

This equation is proved in real cohomology and not known in integral cohomology. Again $\hat{p}_2 = \hat{W}_4{}^2$, where $\hat{W}_4$ is the Euler class of the bundle along the fibres. If $\dim B_\xi = 4$ (and hence $\dim E_\xi = 8$), then

$$7\cdot \hat{W}_4{}^2 = \hat{p}_1{}^2.$$

27.5. *Remark.* The strict multiplicativity of $\{L_j\}$ was proved in 22.9 for bundles $\xi\in\mathfrak{D}$ with $F_\xi = G/U$ ($\operatorname{rank} G = \operatorname{rank} U$) and G as structural group. It was also shown (§ 23) in this special case that the sequence $\{A_j\}$ is strictly multiplicative provided $A(F_\xi)=0$. It might be conjectured that in every fibre bundle $\xi\in\mathfrak{D}$ the vanishing of $A(F_\xi)$ implies that of $A(E_\xi)$. As a consequence, we would have (27.2) that $\{A_j\}$ is strictly multiplicative in every fibre bundle $\xi\in\mathfrak{D}$ with $A(F_\xi)=0$.

28. A uniqueness theorem on the index.

28.1. In this paragraph, we shall prove that the sequence $\{L_j\}$ is essentially the only multiplicative sequence with coefficients in a field of characteristic 0 giving rise to a genus which is multiplicative in fibre bundles. Throughout this paragraph, we keep the notations of 27.1.

Let M be a $4k$-dimensional compact oriented differentiable manifold and p_i its Pontrjagin classes, which may be written formally as elementary symmetric functions:

$$1 + p_1 + \cdots + p_k = (1+\beta_1)\cdots(1+\beta_k).$$

Then the number $s(M)$ is defined by

$$s(M) = (\beta_1{}^k + \cdots + \beta_k{}^k)[M], \qquad \text{(see [19, § 6.3])}.$$

28.2. Lemma. *Let $\xi\in\mathfrak{D}$ be a principal $\boldsymbol{U}(q)$-bundle over a 4-dimensional base space and c_i its Chern classes. If $2q+2 = 4k \geqq 8$, then*

$$s(E_\xi/\boldsymbol{U}(1)\times\boldsymbol{U}(q-1)) = (-q(q+2)c_2 + (\binom{q+1}{2} - 1)c_1{}^2)[B_\xi].$$

For the proof, we use the notations of 15.1. We always take into

account that B_ξ is 4-dimensional, and hence, for example, $c_i = 0$ for $i > 2$ and

(1) $$\pi^*(1 + c_1 + c_2) = (1 + x_1)(1 + x_2) \cdots (1 + x_q).$$

Furthermore

(2) $$x_1^q - x_1^{q-1}\pi^*(c_1) + x_1^{q-2}\pi^*(c_2) = 0.$$

Letting $a = \sum_{j=1}^{q} (x_j - x_1)^{q+1}$, we get by (1) that

(3) $$(-1)^q a = -q \cdot x_1^{q+1} + (q+1)x_1^q \cdot \pi^*(c_1) - \binom{q+1}{2} x_1^{q-1} \cdot \pi^*(c_1^2 - 2c_2).$$

We infer readily from (2) and (3) that

$$(-1)^q a = (q+2)q \cdot x_1^{q-1}\pi^*(c_2) + (1 - \binom{q+1}{2}) \cdot x_1^{q-1} \cdot \pi^*(c_1^2).$$

We may put $a = \rho^*(b)$ and $x_1 = \rho^*(\gamma_1)$. Then the preceding formula yields

(4) $$b = -q(q+2)(-\gamma_1)^{q-1}\sigma^*(c_2) + (\binom{q+1}{2} - 1) \cdot (-\gamma_1)^{q-1}\sigma^*(c_1^2)$$

M will denote the total space of the bundle $\theta = (E_\xi/\boldsymbol{U}(1) \times \boldsymbol{U}(q-1), B_\xi, \boldsymbol{P}_{q-1}(\boldsymbol{C}))$. The tangent bundle of M is the Whitney sum of $\hat{\theta}$, the bundle along the fibres of θ, and of the tangent vector bundle of B_ξ lifted by σ. We have for the total Pontrjagin classes

(5) $$p(M) = p(\hat{\theta}) \cdot \sigma^* p(B_\xi) = p(\hat{\theta}) \cdot (1 + \sigma^* p_1(B_\xi)).$$

In 15.1, one finds a formula for $\rho^* c(\eta')$ which yields

(6) $$\rho^* p(\hat{\theta}) = \prod_{j=1}^{q} (1 + (x_j - x_1)^2).$$

By (5) and (6), we get for $2q + 2 = 4k$

$$s(M) = (b + (\sigma^*(p_1(B_\xi))^k))[M].$$

Since $(p_1(B_\xi))^k = 0$ for $k \geqq 2$, we have $s(M) = b[M]$ which, by (4), completes the proof because the value of $(-\gamma_1)^{q-1}$ on the oriented fibres of θ equals 1.

28.3. We are going to construct a special base sequence for the algebra $\Omega \otimes \boldsymbol{Q}$ of Thom [29]. Consider over $X = \boldsymbol{P}_2(\boldsymbol{C})$ the differentiable principal $\boldsymbol{U}(q)$-bundle $\xi(q)$ which is the Whitney sum of $q - 2$ trivial $\boldsymbol{U}(1)$-bundles and of the two principal $\boldsymbol{U}(1)$-bundles with g and $-g$ respectively as first

Chern classes, where g is the cohomology class dual to a complex projective line imbedded in X. The Chern classes of $\xi(q)$ are

$$c_1 = 0, \qquad c_2 = -g^2.$$

For $2q+2=4k \geqq 8$, let E^{4k} be the $4k$-dimensional manifold fibred with $\boldsymbol{P}_{q-1}(\boldsymbol{C})$ as fibre and associated to $\xi(q)$; i.e.

$$E^{4k} = E_{\xi(q)}/\boldsymbol{U}(1) \times \boldsymbol{U}(q-1), \qquad (2q+2=4k \geqq 8).$$

According to the preceding lemma, we have

$$(7) \qquad s(E^{4k}) = (2k+1)(2k-1) = 4k^2-1 \neq 0.$$

For $k=1$, we put $E^4 = \boldsymbol{P}_2(\boldsymbol{C})$ and then (7) holds also in this case.

By [19, § 6], the sequence $\{E^{4k}\}$, $(k=1,2,3,\cdots)$, of $4k$-dimensional manifolds is a base sequence of the algebra $\Omega \otimes \boldsymbol{Q}$ of Thom; and we have in terms of the usual base sequence $\boldsymbol{P}_{2k}(\boldsymbol{C})$

$$(8) \qquad E^{4k} = (2k-1)\boldsymbol{P}_{2k}(\boldsymbol{C}) + \text{composite terms in the } \boldsymbol{P}_{2j}(\boldsymbol{C}), j<k.$$

28.4. THEOREM. *Let $\{K_r(p_1,\cdots,p_r)\}$ be a multiplicative sequence of polynomials with coefficients in a field of characteristic* 0 *and suppose that the corresponding genus K satisfies the equation $K(E)=K(B)\cdot K(F)$ for all differentiable fibre bundles in $\mathfrak{D}$, or equivalently* (27.2), *that $\{K_r(p_1,\cdots,p_r)\}$ is strictly multiplicative in $\mathfrak{D}$. Put $a=K(\boldsymbol{P}_2(\boldsymbol{C}))$. Then*

$$(9) \qquad K(Y) = a^r \cdot L(Y), \qquad (4r = \dim Y)$$

for all $4r$-dimensional compact oriented differentiable manifolds Y, and moreover

$$(10) \qquad K_r(p_1,\cdots,p_r) = a^r L_r(p_1,\cdots,p_r), \qquad (r=1,2,3\cdots).$$

We prove (9) by induction over r. It is true for $r=1$ since $\boldsymbol{P}_2(\boldsymbol{C})$ generates Ω^4. Suppose it is proved for all Y with $\dim Y < 4r$. The vector space $\Omega^{4r}\otimes\boldsymbol{Q}$ over the rationals is generated by E^{4r} and "composite" manifolds M^{4r} which are cartesian products of lower dimensional manifolds. Since K and L are both multiplicative in cartesian products, (9) is true on the composite manifolds M^{4r} by induction hypothesis, and since K and L are also both multiplicative in differentiable fibre bundles, (9) is true on E^{4r} too (again we have used the induction hypothesis). Thus (9) holds on $\Omega^{4r}\otimes\boldsymbol{Q}$.

This proves (9) in full generality which implies (10), [19, Satz 6.5.1].

Appendix I.

29. The different definitions of the Chern classes.

29.1. *Orientation conventions.* In the n-dimensional complex vector space V with coordinates $z_j = x_j + iy_j$, we take as usual the orientation defined by the order $x_1, y_1, \cdots, x_n, y_n$. This determines also an orientation for complex analytic manifolds as well as for the $2n-1$ dimensional sphere $\boldsymbol{S}_{2n-1}$ of unit vectors with respect to some hermitian metric on V. The image of the fundamental cycle of $\boldsymbol{S}_{2n-1}$ thus defined in $\pi_{2n-1}(\boldsymbol{S}_{2n-1})$, or $H_{2n-1}(\boldsymbol{S}_{2n-1}, \boldsymbol{Z})$, or $H_{2n-1}(V-0, \boldsymbol{Z})$, (0 being the origin in V), and the element of $H^{2n-1}(\boldsymbol{S}_{2n-1}, \boldsymbol{Z})$ or $H^{2n-1}(V-0, \boldsymbol{Z})$ taking the value 1 on it will be called the canonical generator of the corresponding group.

Let $\boldsymbol{W}_{n,n-q+1}$ be the complex Stiefel manifold of ordered systems of $n-q+1$ orthonormal vectors in $\boldsymbol{C}^n$ $(1 \leqq q \leqq n)$. We know that its first non-vanishing homotopy group is in dimension $2q-1$ and is infinite cyclic. Now $\boldsymbol{W}_{n,n-q+1}$ is fibered by $\boldsymbol{W}_{q,1} = \boldsymbol{S}_{2q-1}$, with base $\boldsymbol{W}_{n,n-q}$; the projection assigning to each $(n-q+1)$-frame the $(n-q)$-frame formed by its first $n-q$ elements. The fibre may thus be identified with the set of unit vectors in $\boldsymbol{C}^q$ and its injection in $\boldsymbol{W}_{n,n-q+1}$ induces isomorphisms for the $(2q-1)$-st homotopy or homology or cohomology groups. The element corresponding to the canonical generator previously defined will also be called the canonical generator.

Similarly, let $\boldsymbol{W}^*_{n,n-q+1}$ be the manifold of ordered systems of $n-q+1$ linearly independent vectors in $\boldsymbol{C}^n$; it has $\boldsymbol{W}_{n,n-q+1}$ as a deformation retract; let $e_1, \cdots, e_{n-q}$ be independent vectors, and let V be a q-dimensional subspace supplementary to the space spanned by the e_i's. The subspace U of $\boldsymbol{W}^*_{n,n-q+1}$ made of the systems (f_j), $(j = 1, \cdots, n-q+1)$, for which $f_j = e_j$ $(j \leqq n-q)$ and f_{n-q+1} is in V may be identified with $V-0$. Its injection in the Stiefel manifold is an isomorphism for homotopy or homology in dimension $2q-1$ and we define as before the canonical generator of $H_{2q-1}(\boldsymbol{W}^*_{n,n-q+1}, \boldsymbol{Z})$ and $\pi_{2q-1}(\boldsymbol{W}^*_{n,n-q+1})$.

29.2. *The Hopf fibering.* (x_i), $(1 \leqq i \leqq n+1)$, are the coordinates of $\boldsymbol{C}^{n+1}$ and the homogeneous coordinates in the complex projective space $\boldsymbol{P}_n$. By the Hopf fibering over $\boldsymbol{P}_n$, we mean here $\boldsymbol{C}^{n+1}-0$ endowed with the usual $\boldsymbol{C}^* = \boldsymbol{GL}(n, 1)$ bundle structure. e will denote a hyperplane with the positive orientation or the corresponding homology class and $e^* \in H^2(\boldsymbol{P}_n, \boldsymbol{Z})$ will be the dual cohomology class. Let U_i be the set of points in $\boldsymbol{P}_n$ for

which $x_i \neq 0$, $(1 \leqq i \leqq n+1)$; using the usual conventions for the transition functions of a bundle [19, § 3. 2. a] and of a line bundle associated to a divisor D [19, § 15. 2] we see that in $U_i \cap U_j$ the Hopf fibering is given by $f_{ij} = x_i/x_j$, whereas the bundle $\{e\}$ associated to e is given by $g_{ij} = x_j/x_i$; thus the Hopf fibering is the inverse of $\{e\}$. We recall that the Hopf fibering over $\boldsymbol{P}_n$ is a $2n$-universal bundle for $\boldsymbol{C}^*$ or $\boldsymbol{U}(1)$.

29. 3. *The definitions of Chern classes.* Including the definition (9. 1), there are apparently seven definitions of Chern classes, which we proceed to list now; ${}^ic_j$ will be the j-th Chern class according to the i-th definition, and ${}^ic$ the sum of the ${}^ic_j$.

(1) *The definition* (9. 1) *of this paper.* It may also be formulated in the following way: in the Hopf fibering, we put ${}^1c_1 = -\tau(x)$, where x is the canonical generator of $H^1(\boldsymbol{C}^*, \boldsymbol{Z})$; for a general $\boldsymbol{C}^*$-bundle, we use the characteristic map; for a general $\boldsymbol{GL}(n, C)$ bundle, we go over to the bundle of flags and take the elementary symmetric functions in the Chern classes of the different line bundles in which the lifted bundle decomposes.

(2) *The definition of* [19]: it is quite similar to (1), except that we put ${}^2c_1 = -e^*$ in the Hopf fibering.

(3) *The obstruction definition.* Given a complex vector bundle $(E, B, \boldsymbol{C}^n)$, we consider the associated bundle $(E', B, \boldsymbol{W}_{n,n-q+1})$. The first obstruction to the construction of a cross section (B is supposed to be a complex here) is an element of $H^{2q}(B, \pi_{2q-1}(\boldsymbol{W}_{n,n-q+1}))$. We identify the coefficient group with $\boldsymbol{Z}$ by sending the canonical generator onto 1, and thus get a class ${}^4c_q \in H^{2q}(B, \boldsymbol{Z})$.

This convention was introduced in [20], and was recalled at the beginning of [11] but was not made in [9], where consequently the obstruction classes are defined up to sign only.

(4) *The definition of* [6]: in the Hopf fibering, considered as universal bundle, we put ${}^4c_1 = \tau(x)$, and then proceed as in (1).

(5) *Schubert systems.* Let $\boldsymbol{H}(n, N)$ be the complex Grassmann manifold of n-dimensional subspaces of $\boldsymbol{C}^{n+N}$. It is the base space of the $2N$-universal bundle $(\boldsymbol{U}(n+N)/\boldsymbol{U}(N), \boldsymbol{H}(n, N), \boldsymbol{U}(n))$ for $\boldsymbol{U}(n)$, where $\boldsymbol{U}(N)$, (respectively $\boldsymbol{U}(n)$), is the subgroup of $\boldsymbol{U}(n+N)$, leaving the n first (respectively N last) coordinate vectors fixed. For $n=1$, we have the Hopf fibering. We take as universal ${}^5c_q$ the dual class to the Schubert cycle of dimension $2(nN-q)$ represented by the symbol $(N-1, \cdots, N-1, N, \cdots, N)$,

(q times $N-1$, $(n-q)$ times N). By the intersection properties of Schubert varieties, ${}^5c_q$ is also the cohomology class taking the value 1 on the Schubert cycle $(0,\cdots 0,1,\cdots,1)$ ($(n-q)$ times 0, q times 1), and zero on all other Schubert cycles of Ehresmann's cell decomposition of $\boldsymbol{H}(n,N)$; (Schubert cycles are defined for instance in [9, 10, 11].) This defines ${}^5c$ in the universal bundle; for a general bundle, we take its image by the characteristic map. For $n=1$, the Schubert symbol $(N-1)$ represents the hyperplane of $\boldsymbol{P}_N(\boldsymbol{C})=\boldsymbol{H}(1,N)$. Thus, in the Hopf fibering, we have ${}^5c_1=e^*$.

(6) *Definition by means of differential forms.* This leads to real cohomology classes, defined for differentiable bundles. Let ξ be a differentiable principal $\boldsymbol{U}(n)$-bundle and let Ω_{ij} $(1\leqq i,j\leqq n)$ be the curvature forms of a connexion on E_ξ. We then consider the (mixed) differential form:

$$\Psi=\sum\Psi_q=\det|\mathrm{Id}+(2\pi i)^{-1}\Omega_{ij}|$$

(Ψ_q of degree q; the product in the determinant is of course the exterior product). It defines a form on B_ξ, which is closed. The image of Ψ_q in $H^{2q}(B_\xi,\boldsymbol{R})$ is by definition ${}^6c_q$. This definition is introduced in [9] (our Ψ_q is the Ψ_{n-q+1} of Chern), although in an apparently slightly more restrictive way. Chern considers only bundles of (tangential) orthonormal frames to a hermitian manifold and a special connexion characterized by a property of its torsion tensor [9, p. 111]. However, by a theorem of Weil, whose proof is reproduced in [10, pp. 58-59], the cohomology class of Ψ_q is independent of the particular connexion chosen in ξ.

(7) *Definition by transgression.* ${}^7c_q$ is the image by transgression of the canonical generator of $H^{2q-1}(\boldsymbol{W}_{n,n-q+1},\boldsymbol{Z})$ in the bundle with fiber $\boldsymbol{W}_{n,n-q+1}$ associated to a given complex vector bundle.

The purpose of this Appendix is to prove the

29.4. THEOREM. *Let ${}^ic_j$ be the j-th Chern class of a bundle $(E,B,\boldsymbol{U}(n))$ with respect to the i-th definition $(j=1,\cdots,n;i=1,\cdots,7)$. Then* ${}^1c_j={}^2c_j={}^3c_j=(-1)^j\cdot{}^4c_j=(-1)^j\cdot{}^5c_j=(-1)^j\cdot{}^6c_j=-{}^7c_j$.

29.5. *Remarks.* (a) All these definitions have the naturality property: if $f\colon\xi\to\eta$ is a homomorphism, then $\bar{f}^*({}^ic(\eta))={}^ic(\xi)$, where $\bar{f}\colon B_\xi\to B_\eta$ is induced by f. This is obvious for $i=1,2,4,5,7$, and standard for $i=3$; for $i=6$, it follows by the theorem of Weil quoted above, because if Ω_{ij} are the curvature forms of a connexion $\mathscr{C}$ on E_η, then their images on E_ξ under f will be the curvature forms of the connexion induced from $\mathscr{C}$ by f.

(b) Let a, b $(1 \leqq a, b \leqq 7)$ be given, and assume that ${}^a c_1 = \epsilon \cdot {}^b c_1$ $(\epsilon = \pm 1)$ and that ${}^a c$ obeys duality.[6] Then ${}^b c$ obeys duality if and only if ${}^a c_j = \epsilon^j \cdot {}^b c_j$, $(1 \leqq j \leqq n)$. This is readily seen by using the bundle of flags. Thus ${}^i c$ has the duality property for $i \leqq 6$, but not for $i = 7$. For $i = 1, 2, 4$, the duality property follows immediately from an identity between elementary symmetric functions (see e. g. [6]). In the course of the proof of the theorem we shall *use* the fact that ${}^5 c$ obeys duality, which is proved in [11], and therefore we do not provide a new proof for it. We note in passing that in the introduction of [11], Chern classes are defined as obstructions (with signs) but the proof for duality is carried out for Schubert cocycles. However, our 29.4 shows that the obstruction classes obey duality, a fact for which there is, to our knowledge, no direct proof in the literature.

29.6. LEMMA. *In the Hopf fibering, we have* ${}^7 c_1 = + e^* = - {}^3 c_1$.

In view of a general fact about transgression and obstructions, recalled below (29.7), it is in fact enough to prove one equality, but both may be easily checked directly: As to the first one, we put $a = \sum x_i \cdot \bar{x}_i$ and consider

$$\Omega = (i/2\pi)\,(a^{-1} \cdot \textstyle\sum dx_i \wedge d\bar{x}_i - a^{-2} \cdot \sum x_i \cdot \bar{x}_j\, dx_j \wedge d\bar{x}_i)\,;$$

it is the imaginary part, multiplied by $1/\pi$, of the Fubini metric

$$ds^2 = a^{-1} \cdot \textstyle\sum dx_i \cdot d\bar{x}_i - a^{-2} \cdot \sum x_i \bar{x}_j\, dx_j \cdot d\bar{x}_i. \tag{1}$$

Ω is a closed real form of type $(1,1)$ on $\boldsymbol{P}_n$ and we integrate it on the projective line $\boldsymbol{P}_1$: $x_3 = \cdots = x_{n+1} = 0$ with homogeneous coordinates (x_1, x_2); leaving out $(0,1)$, we replace $\boldsymbol{P}_1$ by the cross section $x_1 = 1$ and get for the integral

$$(i/2\pi) \int_{\boldsymbol{P}_1} (1 + x_2 \cdot \bar{x}_2)^{-2} \cdot dx_2 \wedge d\bar{x}_2 = 1.$$

Hence Ω represents e^*. On the other hand, we have

$$\Omega = (i/2\pi)\, d\bar{\partial} \log a = d(\,(i/2\pi) a^{-1} \cdot \textstyle\sum x_i \cdot d\bar{x}_i),$$

and the restriction of $(i/2\pi)\bar{\partial} \log a$ to the fibre $x_2 = \cdots = x_{n+1} = 0$ is $i(2\pi \bar{x}_1)^{-1} d\bar{x}_1$, whose integral on the positively oriented unit circle is again 1; this proves the first equality.

${}^3 c_1$ is the first obstruction to the construction of a cross section in the Hopf fibering and we only need to know its value on $\boldsymbol{P}_1$. Over this line, we consider the cross section defined (except at $(0,1)$) by $(x_1, x_2) \to (1, x_2/x_1)$.

---

[6] By duality we mean the multiplication theorem 9.7(6).

Around $(0,1)$, we take as product representation of the bundle the one which identifies 1 on the typical fibre with $(x_1/x_2, 1)$; then we see easily that around $(0,1)$, the map $\boldsymbol{P}_1 \to \boldsymbol{C}^*$ which defines the value of the obstruction cochain on a 2 simplex having $(0,1)$ in its interior, is of the form $z \to 1/z$; this value will therefore be -1, and so will be that of the obstruction cochain on $\boldsymbol{P}_1$, hence the second equality.

29.7. *Proof of the theorem.* By the definitions, the lemma and naturality, we have

$$ {}^1c_1 = {}^2c_2 = {}^3c_1 = -{}^4c_1 = -{}^5c_1 = -{}^7c_1 $$

since all these classes are equal to $-e^*$ in the Hopf fibering. For $i = 1, 2, 4, 5$, ${}^ic$ satisfies duality, and we get therefore (see 29.5b)

$$ {}^1c_i = {}^2c_i = (-1)^i \cdot {}^4c_i = (-1)^i \cdot {}^5c_i \qquad (1 \leqq i \leqq n). \tag{2} $$

The equality

$$ {}^3c_j = -{}^7c_j, \qquad (1 \leqq j \leqq n), \tag{3} $$

follows from the more general fact that in a fibre bundle, "transgression is minus obstruction" for a proof of which we refer to [26, § 37.16].

The $2N$-universal bundle for $\boldsymbol{U}(n)$ over $\boldsymbol{H}(n,N)$ is $(\boldsymbol{W}_{n+N,n}, \boldsymbol{H}(n,N), \boldsymbol{U}(n))$ which may also be written as $(\boldsymbol{U}(n+N)/\boldsymbol{U}(N), \boldsymbol{H}(n,N), \boldsymbol{U}(n))$, where $\boldsymbol{U}(N)$, (respectively $\boldsymbol{U}(n)$), is the subgroup of $\boldsymbol{U}(n+N)$ leaving the n first (respectively N last) coordinate vectors fixed. Let (u_{ij}), $(1 \leqq i, j \leqq n+N)$, be the standard coordinates in the matrix space. Following Chern [9], we denote by θ_{ab} the left invariant Maurer-Cartan form on $\boldsymbol{U}(n+N)$ which is equal to du_{ba} (and not du_{ab}) at the neutral element. In these notations, we have

$$ d\theta_{ab} = \sum_1^{n+N} \theta_{ai} \wedge \theta_{ib}; \qquad \theta_{ba} = -\bar{\theta}_{ba}. \tag{4} $$

It is easily seen that for $1 \leqq a, b \leqq n$, the forms are right invariant under $\boldsymbol{U}(N)$ and satisfy

$$ \theta_{ab} \cdot u = \sum_{ij} u_{ia} \theta_{ij} (u^{-1})_{bj} \qquad (u \in \boldsymbol{U}(n), u = (u_{ij})), $$

hence they induce forms on $\boldsymbol{U}(n+N)/\boldsymbol{U}(N)$ which define there a connexion for the $\boldsymbol{U}(n)$-bundle structure. (4) shows that its curvature forms are

$$ \Omega_{ij} = \sum_{k=n+1}^{k=N} \theta_{ik} \wedge \theta_{kj}, \qquad (1 \leqq i, j \leqq n). $$

Thus, by definition

$$\Psi = \sum \Psi_q = \det | \mathrm{Id} + (2\pi i)^{-1}\Omega_{ij} |$$

represents ${}^6c$ in the universal bundle. By a computation which we shall not reproduce, Chern ([9], Chap. II, § 2, [10], p. 77) has shown that Ψ_q is equal to ${}^5c_q$; hence

$$(5) \qquad {}^5c_j = {}^6c_j, \qquad (j = 1, \cdots, n),$$

first in the universal bundle, and then by naturality in all differentiable $U(n)$-bundles.

To conclude the proof, we have to compare the obstruction classes with one of the six other types, and it will be enough to show that

$$(6) \qquad {}^3c_j = (-1)^j \cdot {}^6c_j, \qquad (1 \leqq j \leqq n).$$

We have first

$${}^3c_j = \epsilon_j \cdot {}^6c_j \qquad (\epsilon_j = \pm 1, j = 1, \cdots, n),$$

with ϵ_j depending only on j; by naturality, we have only to prove this in the universal bundle; there it follows from (2), (3), (5), and from the fact that ${}^7c_j$ and ${}^4c_j$ both generate the kernel of $\rho^*(U(j-1), U(n))$ in dimension $2j$, which is infinite cyclic. The proof of this is identical with that of a similar statement on Stiefel-Whitney classes [3, Lemme 5.1] and will be left to the reader.

To determine ϵ_j, it is then enough to compute the 2 classes ${}^3c$ and ${}^6c$ for one bundle with Chern classes not zero or of order 2. To this end, we take the tangent bundle of $\boldsymbol{P}_n$. By [9, p. 118], we have

$$\Psi_j = (2\pi i)^{-j} \binom{n+1}{j} \Lambda^j$$

for the torsionless connexion associated to the Fubini metric, where Λ is the exterior form obtained from the metric (1) by replacing the symmetric products by exterior products; in the notation of 29.6, we have, therefore, $\Omega = i(2\pi)^{-1} \cdot \Lambda$ and

$$\Psi_j = \binom{n+1}{j} (-1)^j \Omega^j.$$

We have seen in the proof of 29.6 that Ω represents e^* and, consequently,

$$(7) \qquad {}^6c_j = \binom{n+1}{j} (-1)^j (e^*)^j, \qquad (1 \leqq j \leqq n),$$

as also follows from 15.1 and (2), (5). On the other hand, a direct con-

struction of vector fields in [9, Theorem 13] shows that

$$ {}^{s}c_j = \binom{n+1}{j}(e^*)^j, \qquad (j=1,\cdots,n), \tag{8} $$

whence $\epsilon_j = (-1)^j$ and (6). Of course we must check that in the proof of (8), the indices of singularities are counted with the proper sign conventions; this presents no difficulty, but for the sake of completeness, we outline Chern's construction. Let

$$ \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_{11} & a_{12} & & a_{1,n+1} \\ & \cdot\ \cdot\ \cdot\ \cdot & & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{n,n+1} \end{pmatrix} $$

be a matrix with constant coefficients and all minors of degree j $(1 \leqq j \leqq n+1)$ different from zero. Let H_j be the j-dimensional projective subspace defined by

$$ \sum_k a_{ik}x_k = 0 \qquad (1 \leqq i \leqq n-j). $$

We denote by $\mathfrak{v}_j$ the vector field on $C^{n+1}-0$ defined by

$$ \mathfrak{v}_j(x) = \sum_k a_{jk}x_k\mathfrak{e}_k, \qquad ((\mathfrak{e}_k) \text{ canonical basis of } C^{n+1}). $$

It is invariant under $x \to a\cdot x$ $(a \in C^*)$ and defines a vector field $\mathfrak{w}_j$ on P_n. The vectors $\mathfrak{w}_j$ $(j \leqq r)$ are dependent at a point P with homogeneous coordinates (x_i) if and only if the $r+1$ vectors $\mathfrak{x} = \sum x_i\mathfrak{e}_i$ and $\mathfrak{v}_1,\cdots,\mathfrak{v}_r$ are dependent at $x=(x_i)$, which is equivalent with the vanishing of $n+1-r$ homogeneous coordinates of P.

Let now j be fixed and put $r=n-j+1$. On H_j, $\mathfrak{w}_1,\cdots,\mathfrak{w}_{r-1}$ are independent everywhere whereas $\mathfrak{w}_1,\cdots,\mathfrak{w}_r$ are dependent at $\binom{n+1}{j}$ points. We use these vector fields to compute the value of ${}^{s}c_j$ on H_j; since we already know that it is equal to $\pm\binom{n+1}{j}$, we have only to show that the singular points have non-negative indices. Let Q be a singular point, and W a neighborhood of Q on H_j. Using the fields $\mathfrak{w}_1,\cdots,\mathfrak{w}_{r-1}$ which are also independent at Q we see immediately that the map $W-Q \to W^*_{n,r}$ leading to the index is homotopic to a complex analytic map of $W-Q$ into a subspace of $W^*_{n,r}$ of the type of the space U introduced in 29.1, and that the resulting map of $W-Q$ in C^j-0 extends analytically to Q and maps it onto the origin; hence it has a positive degree, and the index is $\geqq 0$ according to the conventions of 29.1 and 29.3(3).

29.8. *Remarks.* (a) The obstruction classes ${}^3c_j$ are the obstructions to the construction of *contravariant* vector fields. Hodge [20] uses co-variant vector fields and, by 29.4 and 10.6a, or directly, the resulting classes are our ${}^4c_j$.

(b) According to Hodge [20] and Nakano (Mem. Coll. Sci. Kyoto 29 (1955), 145-149), the canonical classes of Eger-Todd are to be identified with the Schubert classes ${}^5c_j$.

(c) The lack of sign conventions for obstruction classes in [9] leads to a slight inaccuracy for the Chern classes of $\boldsymbol{P}_n$; Theorem 13 gives $c_j = \binom{n+1}{j}(e^*)^j$ and Theorem 12 gives the class of Ψ_j; as we have seen, these differ by $(-1)^j$.

29.9. Finally, to be complete, we list some properties or alternate definitions of the first Chern class. For the notations, and concepts used here, see [19].

(a) Let $\boldsymbol{C}^*_c$ be the sheaf of germs of continuous $\boldsymbol{C}^*$-valued functions on the space B. A complex line bundle over B is represented by an element $\xi \in H^1(B, \boldsymbol{C}^*_c)$ and we have

$$ {}^1c_1 = \delta\xi, $$

where δ is the coboundary operator $H^1(B, \boldsymbol{C}^*_c) \to H^2(B, \boldsymbol{Z})$ associated to the exact sequence $0 \to \boldsymbol{Z} \to \boldsymbol{C}_c \xrightarrow{e} \boldsymbol{C}^*_c \to 0$, where e is the exponential map [19, § 4.3.1].

(b) Let V be an oriented m-dimensional manifold, B an oriented $(m-2)$-dimensional submanifold, η the normal bundle oriented in such a way that orientation of B plus orientation of η gives the orientation of V. It has then a complex structure compatible with its orientation, determined up to isomorphism; its class ${}^1c_1$ is dual to the homology class defined by B [19, § 4.8.1].

(c) Kodaira has introduced the following definition for the Chern class c_1 of a holomorphic principal $\boldsymbol{C}^*$-bundle $\xi = (E, B, \boldsymbol{C}^*, \pi)$. Let (U_j) be a covering by coordinate neighborhoods, z_j the coordinate of the standard fibre over U_j, (f_{jk}) the transition functions, (a_j) a cross section of the bundle with fibre $\boldsymbol{R}^+$ defined by the transition functions $f_{jk} \cdot \bar{f}_{jk}$. Then $c_1(\xi)$ is the class of the form $\gamma = (i/2\pi)\partial\bar{\partial} \log a_j$. *This class is equal to* ${}^1c_1$.

Proof. We have $\pi^*(\gamma) = d\psi$, where ψ is a 1-form over E with the local

representation $(-i/2\pi)\bar{\partial}\log(\bar{z}_j/a_j)$ over U_j; the restriction of ψ to a fibre is $(-i/2\pi)\bar{z}_j^{-1}d\bar{z}_j$ and its integral over the positively oriented unit circle is -1. Thus the Kodaira class is equal to $-\tau(x)$, where x is the canonical generator of $H^1(\boldsymbol{C}^*, \boldsymbol{Z})$, and is equal to ${}^1c_1$ by 29.4.

(d) On a complex manifold B of complex dimension n, the *canonical bundle* K is the line bundle of exterior forms of type $(n, 0)$, i.e. the bundle of n-forms on the tangent bundle. By (10.6a, b), its Chern class is $-{}^1c_1(\theta)$, where θ is the tangential bundle. In particular, the determinant g of a positive non-degenerate hermitian metric provides a section of the bundle with fibre $\boldsymbol{R}^+$ and transition functions $|f_{jk}|^2$, (f_{jk} being the transition functions of K). Thus the Ricci form

$$(-i/2\pi)\partial\bar{\partial}\log g,$$

where $R_{\alpha\bar{\beta}} = -\partial^2 \log g/\partial z_\alpha \partial \bar{z}_\beta$ is the Ricci tensor, represents ${}^1c_1(\theta)$ (see Kodaira, Annals of Math. 60 (1954), 28-48).

Appendix II.

30. Pontrjagin classes.

30.1. *Notation.* $\operatorname{Tors} A$ is the torsion subgroup of the commutative group A, and $\operatorname{Tors}_p A$ its p-primary component.

Let V be a vector space graded by finite dimensional subspaces V^i $(i \geqq 0)$. By $P(V, t)$, we denote its Poincaré polynomial

$$P(V, t) = \sum \dim V^i \cdot t^i,$$

and for a topological space X, we write $P_p(X, t)$ for $P(H^*(X, \boldsymbol{Z}_p), t)$.

f^*_p and $f^*_{\boldsymbol{Z}}$ denote the homomorphism of cohomology rings over $\boldsymbol{Z}_p$ and $\boldsymbol{Z}$ induced by a continuous map f.

Let ξ be a bundle with connected fibres, and A a commutative group. Then $T^i(F_\xi, A)$ or simply $T^i{}_\xi$ denotes the subgroup of transgressive elements in $H^i(F_\xi, A)$. We recall that the transgression τ_ξ is a homomorphism of $T^i{}_\xi$ into the quotient of $H^{i+1}(B_\xi, A)$ by a subgroup which will be denoted by $L^{i+1}(B_\xi, A)$ or $L^{i+1}{}_\xi$; we have $L^2{}_\xi = 0$.

30.2. *Cohomology* mod p *of* $B_{O(n)}$ *and* $B_{SO(n)}$. Let G be a compact Lie group, T a maximal torus. The ring of invariants of $W(G)$ operating in the usual way in $H^*(B_T, \boldsymbol{Z})$ is denoted by I_G. If $G = \boldsymbol{SO}(2n+1)$, $\boldsymbol{O}(2n+1)$, $\boldsymbol{O}(2n)$, (respectively $G = \boldsymbol{SO}(2n)$), and if (y_j) is the base induced by trans-

gression in (E_G, B_T, T) from the basis of $H^1(T,\boldsymbol{Z})$ discussed in § 9, then $W(G)$ is the group of permutations of the y_i's combined with an arbitrary (respectively even) number of changes of signs, and consequently $I_G = S(y_1^2, \cdots, y_n^2)$, (respectively is generated by $S(y_1^2, \cdots, y_n^2)$ and by the product of the y_i's).

PROPOSITION. *Let $G = \boldsymbol{SO}(n)$ or $\boldsymbol{O}(n)$, let $\boldsymbol{T}$ be its standard maximal torus, and let $\boldsymbol{Q}$ be the subgroup of diagonal matrices. Then*

(a) *For $p \neq 2$, $\rho^*_p(\boldsymbol{T}, G)$ maps $H^*(B_G, \boldsymbol{Z}_p)$ isomorphically onto $I_G \otimes \boldsymbol{Z}_p$.*

(b) *$\rho^*_2(\boldsymbol{Q}, \boldsymbol{O}(n))$ maps $H^*(B_{\boldsymbol{O}(n)}, \boldsymbol{Z}_2)$ isomorphically onto $S(u_1, \cdots, u_n)$, where (u_i) is a suitable basis of $H^1(B_{\boldsymbol{Q}}, \boldsymbol{Z}_2)$.*

For (b), see [3, Théorème 5], where a similar statement is also proved for $\boldsymbol{SO}(n)$. For $G = \boldsymbol{SO}(n)$, the assertion (a) is proved in [2, § 29]. For $G = \boldsymbol{O}(n)$, it follows from the more general

30.3. PROPOSITION. *Let G be a compact Lie group, G_0 its largest connected subgroup, T a maximal torus. If $H^*(G_0, \boldsymbol{Z})$ has no p-torsion and if the order of G/G_0 is not divisible by p, then $\rho^*_p(T, G)$ is an isomorphism of $H^*(B_G, \boldsymbol{Z}_p)$ onto $I_G \otimes \boldsymbol{Z}_p$.*

For $p = 0$, see [2, Prop. 27.1]. For p prime, the proof is practically identical, in view of the absence of torsion on G_0/T, (14.2), and is left to the reader.

30.4. *A remark on the Bockstein homomorphism.* Let X be a space with finitely generated integral cohomology groups. Let r_i be the number of cyclic direct summands of the p-primary component of $H^i(X, \boldsymbol{Z})$. Then by the universal coefficient formula

$$P_p(X,t) - P_0(X,t) = (1 + 1/t) \sum r_i \cdot t^i.$$

Let β_p be the Bockstein homomorphism attached to the exact sequence

$$0 \to \boldsymbol{Z} \xrightarrow{\alpha} \boldsymbol{Z} \to \boldsymbol{Z}_p \to 0 \qquad (\alpha(x) = px, x \in \boldsymbol{Z})$$

followed by reduction mod p. Clearly $\beta_p \circ \beta_p = 0$, and

$$s_i = \dim \beta_p(H^{i-1}(X, \boldsymbol{Z}_p))$$

is the number of torsion coefficients of $\operatorname{Tors}_p H^i(X, \boldsymbol{Z})$ which are equal to p. Thus we see:

LEMMA. $\mathrm{Tors}_p H^*(X, \boldsymbol{Z})$ *consists of elements of order* p *if and only if*

$$P_p(X,t) - P_0(X,t) = (1+1/t)P(\beta_p(H^*(X,\boldsymbol{Z}_p)),t).$$

When this is the case, the kernel of β_p *is the reduction* mod p *of* $H^*(X,\boldsymbol{Z})$, *and its image is the reduction* mod p *of* $\mathrm{Tors}_p H^*(X,\boldsymbol{Z})$.

We recall that β_p is an antiderivation and that $\beta_2 = Sq^1$.

30.5. *Integral cohomology of* $B_{O(n)}$ *and* $B_{SO(n)}$. In this section, we shall prove that the torsion elements of the cohomology of these classifying spaces are all of order 2; first we insert a remark to be used in the proof.

Let H be an anticommutative graded algebra with unit over a field K, with $H^0 = K$, and let D be an antiderivation on H, raising degrees by one, of square zero. Let A be a graded subspace stable under D. We denote by N_A, M_A, I_A, J_A, respectively, the kernel of D in A, a graded supplementary subspace to N_A in A, the image of A under D, a graded supplementary subspace to I_A in N_A. Since D increases degrees by one and is an isomorphism of M_A onto I_A, we have

$$P(A,t) = (1+1/t)P(I_A,t) + P(J_A,t). \tag{1}$$

Let now B be a second graded subspace stable under D, linearly disjoint from A over K; i.e., such that the subspace $A\cdot B$ spanned by the products $a\cdot b$ $(a\in A, b\in B)$ is isomorphic to $A\otimes B$ under the natural map $a\otimes b \to a\cdot b$. Using the previous notations, we have, as an elementary special case of the Künneth formula

$$P(J_{A\cdot B},t) = P(J_A,t)\cdot P(J_B,t). \tag{2}$$

PROPOSITION. *The torsion elements of* $H^*(B_{O(n)},\boldsymbol{Z})$ *and* $H^*(B_{SO(n)},\boldsymbol{Z})$ *are of order* 2.

It follows from 30.2 that these spaces have only 2-torsion. By 30.4, there remains to prove that for $G = \boldsymbol{SO}(n), \boldsymbol{O}(n)$, we have

$$P_2(B_G,t) - P_0(B_G,t) = (1+1/t)P(Sq^1(H^*(B_G,\boldsymbol{Z}_2)),t). \tag{3}$$

We have

$$\begin{aligned} &H^*(B_{SO(n)},\boldsymbol{Z}_2) = \boldsymbol{Z}_2[w_2,\cdots,w_n],\ Sq^1 w_i = (i+1)w_{i+1} \\ &H^*(B_{O(n)},\boldsymbol{Z}_2) = \boldsymbol{Z}_2[w_1,\cdots,w_n],\ Sq^1 w_i = w_1 w_i + (i+1)w_{i+1} \end{aligned} \tag{4}$$

(w_i = i-th Stiefel-Whitney class, $i \leq n$, $w_{n+1} = 0$), (see e.g. [3]). We first consider $\boldsymbol{SO}(n)$. By the foregoing, we may write

We put

$$H^*(B_{\mathbf{O}(2m+1)}, \mathbf{Z}_2) = A_0 \otimes A_1 \otimes \cdots \otimes A_m,$$
$$H^*(B_{\mathbf{O}(2m)}, \mathbf{Z}_2) = A'_0 \otimes A_1 \otimes \cdots \otimes A_{m-1},$$

where

$$A_i = \mathbf{Z}_2[w^*_{2i}, w^*_{2i+1}] \qquad (1 \leqq i \leqq m),$$
$$A_0 = \mathbf{Z}_2[w^*_1] = \mathbf{Z}_2[w_1],$$
$$A'_0 = \mathbf{Z}_2[w^*_1, w^*_{2m}] = \mathbf{Z}_2[w_1, w_{2m}].$$

These are stable under cup-product and Sq^1, and we have as above

$$P(J_{A_i}, t) = (1 - t^{4i})^{-1}, \qquad (1 \leqq i \leqq m).$$

In A_0, the kernel of Sq^1 is spanned by w_1^{2s} $(s \geqq 0)$; and the image by w_1^{2s} $(s \geqq 1)$; hence $P(J_{A_0}, t) = 1$. Let us now prove that

$$(5) \qquad P(J_{A'_0}, t) = (1 - t^{2m})^{-1}.$$

We have

$$Sq^1(w_1^s \cdot w_{2m}^t) = (s + t) w_1^{s+1} w_{2m}^t$$

which shows that the monomials $w_1^s w_{2m}^t$ with $s + t$ even (respectively $s + t$ even and $s > 0$) span $N_{A'_0}$ (respectively $I_{A'_0}$). Thus we may take the elements w_{2m}^t (t even) as a base for $J_{A'_0}$, and this proves (5). The remainder of the proof of (3) for $\mathbf{O}(n)$ is then the same as for $\mathbf{SO}(n)$.

30.6. Corollary. *Let $G = \mathbf{O}(n)$ or $\mathbf{SO}(n)$. Then the kernel of Sq^1 on $H^*(B_G, \mathbf{Z})$ is the reduction* mod 2 *of $H^*(B_G, \mathbf{Z})$ and its image is the reduction* mod 2 *of* Tors $H^*(B_G, \mathbf{Z})$. *An element of $H^*(B_G, \mathbf{Z})$ is completely determined by its canonical images in $H^*(B_G, \mathbf{R})$ and $H^*(B_G, \mathbf{Z}_2)$.*

The first assertion follows from 30.4 and 30.5. The second one is an elementary fact about spaces with torsion elements of order 2 only.

In connection with the integral cohomology of $B_{\mathbf{O}(n)}$ and $B_{\mathbf{SO}(n)}$, let us also mention the following

30.7. Proposition. *Let $G = \mathbf{O}(n)$, $\mathbf{SO}(n)$ and let T be a maximal torus of G. Then $\rho^*_Z(T, G)$ maps $H^*(B_G, \mathbf{Z})$ onto I_G; its kernel is the torsion subgroup of $H^*(B_G, \mathbf{Z})$.*

We have seen in 9.3 that $S(y_1^2, \cdots, y_m^2)$, $(m = [n/2])$, is contained in $\rho^*_Z(T, G)$, which proves our statement for $G = \mathbf{SO}(2m+1)$, $\mathbf{O}(2m+1)$, $\mathbf{O}(2m)$. For $G = \mathbf{SO}(2m)$, we have to know moreover that $\rho^*_Z(T, \mathbf{SO}(2m))$ contains the product of the y_j's, but this follows from 9.5.

30.8. *Pontrjagin classes.* We follow the notations of 9.2, 9.3. By 30.6, the equalities

(6) $$\rho^*_0(T,G)(\bar{p}) = \Pi(1+y_i^2), \qquad (G = \boldsymbol{O}(n), \boldsymbol{SO}(n)),$$

(7) p_i (respectively $p_{i+\frac{1}{2}}$) reduced mod 2, is equal to $w_{2i}{}^2$ (respectively $w_{2i+1}{}^2$),

completely characterize the integral Pontrjagin classes. (6), over the integers, follows from 9.1, 9.3, 9.4. It implies that $p_{i+\frac{1}{2}}$ is a torsion element. (7) needs only to be proved for $G = \boldsymbol{O}(n)$ and, in view of 30.2(b), will follow from

(8) $$\rho^*_2(\boldsymbol{Q}(n), \boldsymbol{O}(n))(\bar{p}) = \Pi(1+u_j^2).$$

We have

$$\rho^*_2(\boldsymbol{Q}(n), \boldsymbol{O}(n))(\bar{p}) = \rho^*_2(\boldsymbol{Q}(n), \boldsymbol{U}(n))(c) = \rho^*_2(\boldsymbol{Q}(n), \boldsymbol{T}')(\Pi(1+x_i))$$

where $\boldsymbol{T}'$ is the subgroup of diagonal matrices of $\boldsymbol{U}(n)$ and (x_i) is the standard basis of $H^2(B_{T'}, \boldsymbol{Z})$, and therefore (8) follows from [4, § 11]:

$$\rho^*_2(\boldsymbol{Q}(n), \boldsymbol{T}')(x_i) = u_i^2 \qquad (1 \leqq i \leqq n).$$

30.9. *Remark on integral Stiefel-Whitney classes.* It follows also from 9.5, 30.6, (6), (7) that for an $\boldsymbol{SO}(2m)$-bundle, we have

(9) $$p_m = W_{2m}{}^2,$$

both sides being considered as integral classes. The relations $w_{2i+1} = Sq^1 w_{2i}$ for $\boldsymbol{SO}(n)$-bundles and (30.6), show that the universal w_{2i+1} is the reduction mod 2 of a uniquely determined element

$$W_{2i+1} \in H^{2i+1}(B_{SO(n)}, \boldsymbol{Z})$$

of order 2, the *integral $2i+1$-th Stiefel-Whitney class,* and that we also have

$$p_{i+\frac{1}{2}} = (W_{2i+1})^2$$

over the integers.

30.10. *Pontrjagin classes and transgression.* As usual, $V_{n,k}$ denotes the Stiefel-manifold of orthonormal k-frames in euclidean n-space. We recall [2, § 10] that for n odd, $H^j(V_{n,n-2i+1}, \boldsymbol{Z})$ is equal to $\boldsymbol{Z}$ for $j = 0, 4i-1$, to $\boldsymbol{Z}_2$ for j even running from $2i$ to $4i-2$, and is zero for the other values of j which are $\leqq 4i-1$. We denote by v_i a generator of $H^{4i-1}(V_{n,n-2i+1}, \boldsymbol{Z})$.

The first non-vanishing integral cohomology group of strictly positive dimension of the complex Stiefel manifold $\boldsymbol{W}_{n,n-2i+1}$ is of dimension $4i-1$ and is infinite cyclic. We denote its canonical generator (see 29.1) by t_i.

The inclusion of $\boldsymbol{O}(n)$ in $\boldsymbol{U}(n)$ induces a natural injective map of $\boldsymbol{V}_{n,k}=\boldsymbol{O}(n)/\boldsymbol{O}(n-k)$ into $\boldsymbol{W}_{n,k}=\boldsymbol{U}(n)/\boldsymbol{U}(n-k)$.

LEMMA. *Let n be odd, and $\lambda_{n,i}$ be the natural inclusion of $\boldsymbol{V}_{n,n-2i+1}$ in $\boldsymbol{W}_{n,n-2i+1}$. Let v_i and t_i be defined as above. Then $\lambda^*_{n,i}(t_i)=\pm 2v_i$.*

This lemma will be proved in the next section. Let ξ be a principal $\boldsymbol{O}(n)$-bundle, and ξ' be its complex extension. The given homomorphism of ξ into ξ' induces in a natural way a homomorphism $\alpha\colon \eta\rightarrow\eta'$ of the associated bundles with respective typical fibres $\boldsymbol{V}_{n,n-2i+1}$ and $\boldsymbol{W}_{n,n-2i+1}$. By the transgression definition (29.3(7)), we have $c_{2i}=-\tau_{\eta'}(t_i)$. Hence 29.4 and the lemma imply the

THEOREM. *Let n be odd and t_i be the canonical generator of $H^{4i-1}(\boldsymbol{W}_{n,n-2i+1},\boldsymbol{Z})$ and choose $v_i\in H^{4i-1}(\boldsymbol{V}_{n,n-2i+1},\boldsymbol{Z})$ such that $2v_i=\lambda^*_{n,i}(t_i)$. Let ξ be a principal $\boldsymbol{O}(n)$-bundle, η the associated bundle with fibre $\boldsymbol{V}_{n,n-2i+1}$. Then $p_i(\xi)=(-1)^{i+1}\tau_\eta(2v_i)$* modulo *$L^{4i}{}_\eta$.*

For the notation $L^{4i}{}_\eta$, see 30.1. Since the cohomology groups of $\boldsymbol{V}_{n,n-2i+1}$ in positive dimensions $<4i-1$ are 2-groups, the spectral sequence definition of $L^{4i}{}_\eta$ [2, § 5] shows that $L^{4i}{}_\eta$ is a 2-group, so that the theorem characterizes p_i up to 2-torsion. We remark also that v_i itself is not universally transgressive (see following proof).

Let n be odd and β be the natural projection of E_ξ onto $E_\eta=E_\xi/\boldsymbol{O}(2i-1)$. Then we have of course

$$p_i(\xi)=(-1)^{i+1}\tau_\xi(\beta^*(2v_i))\quad \text{mod } L^{4i}{}_\xi.$$

By [2, § 10], $\beta^*(v_i)$ generates a direct summand of $H^{4i-1}(\boldsymbol{O}(n),\boldsymbol{Z})$ or of $H^{4i-1}(\boldsymbol{SO}(n),\boldsymbol{Z})$.

30.11. *Proof of the lemma.* We first consider the case where $n=2i+1$ and denote by ξ the universal bundle for $\boldsymbol{O}(2i+1)$, by ξ' its complex extension, by η and η' the associated bundles with fibres $\boldsymbol{V}_{2i+1,2}$ and $\boldsymbol{W}_{2i+1,2}$ and by α the natural map of η in η'. We have $H^*(\boldsymbol{V}_{2i+1,2},\boldsymbol{Z}_2)=\wedge(h_{2i-1},h_{2i})$, with $Sq^1h_{2i-1}=h_{2i}$ and $\tau_\eta(h_{2i-1})=w_{2i}$, $\tau_\eta(h_{2i})=w_{2i+1}$ (see for instance [3]); this implies easily that $h_{2i-1}\cdot h_{2i}$ is not universally transgressive. Since $h_{2i-1}\cdot h_{2i}$ is the reduction mod 2 of v_i, the latter is not universally transgressive in integral cohomology. For $\boldsymbol{V}_{2i+1,2}$, we have $H^0=H^{4i-1}=\boldsymbol{Z}$, $H^{2i}=\boldsymbol{Z}_2$ (see e.g. [2], § 10), therefore, the non-zero terms in the spectral sequence of η over the integers have fibre degrees 0, $2i$, $4i-1$ and those with

fibre degree $2i$ have order 2. Therefore $2t_i$ is universally transgressive and $L^{4i}{}_\eta$ consists of elements of order 2.

We know now that $2t_i$ generates $T^{4i-1}(\boldsymbol{V}_{2i+1,2},\boldsymbol{Z})$; this group contains necessarily $\lambda^*{}_{2i+1,i}(v_i)$ since v_i is transgressive in η'. Thus we have $\lambda^*{}_{2i+1,i}(v_i)=2k\cdot t_i$ for some integer k, hence also

$$p_i=\pm k\tau_\eta(2t_i) \quad \mathrm{mod}\, L^{4i}{}_\eta.$$

Let $\boldsymbol{T}$ be the standard maximal torus of $\boldsymbol{O}(2i+1)$. Then, in the notation of 9.3, we get from (1) in 9.3 and from the fact that $L^{4i}{}_\eta$ is a 2-group:

$$y_1{}^2\cdot\cdots\cdot y_i{}^2=\pm k\rho^*{}_Z(\boldsymbol{T},\boldsymbol{O}(2i+1))(\tau_\eta(2t_i)).$$

Since $H^*(B_T,\boldsymbol{Z})$ is the ring of polynomials in the y_j's, this yields $k=\pm 1$, and the lemma for $n=2i+1$.

In the general case, we consider the commutative diagram

$$\begin{tikzcd} \boldsymbol{V}_{n,n-2i+1} \arrow[r, "\lambda_{n,i}"] & \boldsymbol{W}_{n,n-2i+1} \\ \boldsymbol{V}_{2i+1,2} \arrow[u, "\mu"] \arrow[r, "\lambda_{2i+1,i}"] & \boldsymbol{W}_{2i+1,2}, \arrow[u, "\nu"'] \end{tikzcd}$$

where μ, ν are the injection of a fibre in the standard fiberings. It follows from §§ 9, 10 in [2] that μ^*, ν^* are isomorphisms in dimension $4i-1$; therefore the general case of the lemma follows by commutativity of the above diagram from the particular case already proved.

30.12. *A property of* $\rho^*{}_Z(\boldsymbol{O}(r),\boldsymbol{O}(n))$. We end this appendix by proving that $\rho^*{}_Z(\boldsymbol{O}(r),\boldsymbol{O}(n))$ is surjective $(r\leqq n)$, a fact which is useful in the discussion of relative Pontrjagin classes (see M. Kervaire, Amer. J. Math. 79 (1957)).

LEMMA. *Let X, Y be two spaces with finitely generated integral cohomology groups and $f\colon X\to Y$ be a continuous map. We assume:*

(a) *The orders of the torsion elements of $H^*(X,\boldsymbol{Z})$ and $H^*(Y,\boldsymbol{Z})$ are square free.*

(b) *$f^*{}_0$ is surjective.*

(c) *For all primes p, $f^*{}_p$ is a surjective map for the kernels of the Bockstein maps β_p* (see 30.4).

Then $f^*{}_Z$ is surjective.

Let M_i be the image of $H^i(Y,\boldsymbol{Z})$ under f^*. By (b), it has a finite index, say g_i, in $H^i(X,\boldsymbol{Z})$. In view of (30.4), the assumptions (a), (c) imply that

$$f^*\colon H^i(Y,\boldsymbol{Z})\otimes \boldsymbol{Z}_p \to H^i(X,\boldsymbol{Z})\otimes \boldsymbol{Z}_p \qquad (i\geqq 0, p \text{ prime})$$

is surjective, or in other words, that

$$H^i(X,\boldsymbol{Z}) = p\cdot H^i(X,\boldsymbol{Z}) + M_i,$$

hence, by iteration,

$$H^i(X,\boldsymbol{Z}) = g_i\cdot H^i(X,\boldsymbol{Z}) + M_i = M_i.$$

PROPOSITION. *The homomorphism $\rho^*_Z(\boldsymbol{O}(r),\boldsymbol{O}(n))$, $(r\leqq n)$, is surjective.*

By (30.5), $B_{\boldsymbol{O}(r)}$ and $B_{\boldsymbol{O}(n)}$ satisfy (a) of the lemma.

It follows from (9.3) and (30.2) that $H^*(B_{\boldsymbol{O}(n)},\boldsymbol{Z}_p)$ is the ring of polynomials in the universal Pontrjagin classes $(i\geqq 1)$ for $p\neq 2$. Since these are preserved under the natural inclusion $\boldsymbol{O}(r)\subset\boldsymbol{O}(n)$ (see 9.7), it follows that $\rho^*_p(\boldsymbol{O}(r),\boldsymbol{O}(n))$ is surjective for $p\neq 2$. This shows that (b) is fulfilled and also, in view of (30.2), (30.5), that (c) is true for $p\neq 2$. Thus, in order to derive the proposition from the lemma, there remains to show that

(10) $\rho^*_2(\boldsymbol{O}(r),\boldsymbol{O}(n))$ *is surjective for the kernels of Sq^1.*

We write ρ^* for $\rho^*_2(\boldsymbol{O}(r),\boldsymbol{O}(n))$, denote by w_i (respectively $\bar{w}_i$) the universal Stiefel-Whitney classes for $\boldsymbol{O}(r)$- (respectively $\boldsymbol{O}(n)$-) bundles and define w^*_i, $\bar{w}^*_i$ as in the proof of (3).

The assertion (10) is clearly true on any subalgebra $A\subset H^*(B_{\boldsymbol{O}(n)},\boldsymbol{Z}_2)$ which is stable under Sq^1 and mapped injectively by ρ^*; the latter is given by

$$\rho^*(\bar{w}_i)=w_i,\quad \rho^*(\bar{w}^*_i)=w^*_i,\quad (i\leqq r),\quad \rho^*(\bar{w}_j)=0\quad (j>r).$$

Therefore, by (4), this applies to

$$A=\boldsymbol{Z}_2[\bar{w}_1,\cdots,\bar{w}_i]\quad (i\leqq r, i\text{ odd}),\quad \boldsymbol{Z}_2[\bar{w}_1,\cdots,\bar{w}_{r-1},\bar{w}_r^2]\qquad (r\text{ even}),$$
$$\boldsymbol{Z}_2[\bar{w}_1^2,\bar{w}^*_2,\cdots,\bar{w}^*_{r-1},\bar{w}_r^2]\quad (r\text{ even}).$$

This establishes (10) for r odd; for $r=2m$ even, it reduces its proof to that of the following statement: given

$$x=w_{2m}\cdot P+Q,\ Sq^1x=0,\ (P,Q\in\boldsymbol{Z}_2[w_1,\cdots,w_{2m-1},w_{2m}^2]),$$

there exists $y\in H^*(B_{\boldsymbol{O}(n)},\boldsymbol{Z}_2)$ with the properties

$$Sq^1 y = 0, \qquad \rho^*(y) = x.$$

$Sq^1 x = 0$ gives

$$w_{2m}(w_1 P + Sq^1 P) + Sq^1 Q = 0$$

and, since $\mathbf{Z}_2[w_1, \cdots, w_{2m-1}, w_{2m}{}^2]$ is stable under Sq^1,

$$w_1 P + Sq^1 P = Sq^1 Q = 0.$$

We may write

$$P = w_1 R + S, \qquad (R, S \in \mathbf{Z}_2[w_1{}^2, w^*{}_2, \cdots, w^*{}_{2m-1}, w_{2m}{}^2].$$

Hence

$$Sq^1 P = w_1{}^2 R + w_1 \cdot Sq^1 R + Sq^1 S,$$

$$0 = w_1 P + Sq^1 P = w_1(S + Sq^1 R) + Sq^1 S,$$

and, as before,

$$S + Sq^1 R = Sq^1 S = 0.$$

Now let $\bar{P}, \bar{Q}, \bar{R} \in H^*(B_{O(n)}, \mathbf{Z}_2)$ be the elements obtained from P, Q, R by barring the w_i's. Then a trivial computation shows that

$$y = \bar{w}_{2m} \cdot \bar{P} + \bar{Q} + \bar{w}_{2m+1}\, \bar{R}$$

has the desired properties.

THE INSTITUTE FOR ADVANCED STUDY, PRINCETON
AND
UNIVERSITY OF BONN, GERMANY.

REFERENCES.

[1] A. Borel, "Le plan projectif des octaves et les sphères comme espaces homogènes," *Comptes Rendus des Séances de l'Académie des Sciences*, Paris, vol. 230 (1950), pp. 1378-1380.

[2] ———, "Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts," *Annals of Mathematics*, vol. 57 (1953), pp. 115-207.

[3] ———, "La cohomologie mod 2 de certains espaces homogènes," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 165-191.

[4] ———, "Sur l'homologie et la cohomologie des groupes de Lie compacts connexes," *American Journal of Mathematics*, vol. 76 (1954), pp. 273-342.

[5] ———, "Kählerian coset spaces of semi-simple Lie groups," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 40 (1954), pp. 1147-1151.

[6] ——— and J-P. Serre, "Groupes de Lie de puissances réduites de Steenrod," *American Journal of Mathematics*, vol. 75 (1953), pp. 409-448.

[7] ——— and J. de Siebenthal, "Sur les sous-groupes fermés de rang maximum des groupes de Lie compacts connexes," *Commentarii Mathematici Helvetici*, vol. 23 (1949), pp. 200-221.

[7a] ——— and A. Weil, "Représentations linéaires et espaces homogènes kähleriens des groupes de Lie compacts," *Séminaire Bourbaki*, May 1954 (Exposé by J-P. Serre).

[7b] R. Bott, "Homogeneous vector bundles," *Annals of Mathematics*, vol. 66 (1957), pp. 203-248.

[8] E. Cartan, "La géométrie des groupes simples," *Annali di Matematica*, vol. 4 (1927), pp. 209-256, vol. 5 (1928), pp. 253-260.

[9] S. S. Chern, "Characteristic classes of hermitian manifolds," *Annals of Mathematics*, vol. 47 (1946), pp. 85-121.

[10] ———, "Topics in differential geometry," *Notes, Institute for Advanced Study*, Princeton, 1951.

[11] ———, "On the characteristic classes of complex sphere bundles and algebraic varieties," *American Journal of Mathematics*, vol. 75 (1953), pp. 565-597.

[12] ———. F. Hirzebruch, J-P. Serre, "On the index of a fibered manifold," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 587-596.

[13] E. B. Dynkin, "The structure of semi-simple Lie algebras," *Uspehi Matematiceskih Nauk* (*N. S.*), vol. 2 (1947), pp. 59-127, translated in *American Mathematical Society Translations* 17, 1950.

[14] A. Frölicher, "Zur Differentialgeometrie der komplexen Strukturen," *Mathematische Annalen*, vol. 129 (1955), pp. 50-95.

[15] F. Hirzebruch, "On Steenrod's reduced powers, the index of inertia, and the Todd genus," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 39 (1953), pp. 951-956.

[16] ———, "Todd arithmetic genus for almost complex manifolds," "On Steenrod's reduced powers in oriented manifolds," "The index of an oriented manifold and the Todd genus of an almost complex manifold," *Notes, Princeton University*, 1953.

[17] ———, "Über die quaternionalen projektiven Raüme," *Bayerische Akademie der Wissenschaften* (1954), pp. 301-312.

[18] ———, "Some problems on differentiable and complex manifolds," *Annals of Mathematics*, vol. 60 (1954), pp. 213-236.

[19] ———, "Neue topologischen Methoden in der algebraischen Geometrie," *Ergebnisse der Mathematik und ihrer Grenzgebiete* (*N. F.*), Heft 9, Berlin 1956.

[20] W. V. D. Hodge, "The characteristic classes on algebraic varieties," *Proceedings of the London Mathematical Society*, (3) vol. 1 (1951), pp. 138-151.

[21] H. Hopf und H. Samelson, "Ein Satz über die Wirkungsräume geschlossener Liescher Gruppen," *Commentarii Mathematici Helvetici*, vol. 13 (1940-41), pp. 240-251.

[22] K. Kodaira, "On a differential-geometric method in the theory of analytic stacks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 39 (1953), pp. 1268-1273.

[23] "Groupes et algèbres de Lie," *Séminaire S. Lie, Notes,* Paris, 1954.

[24] W. Rohlin, "New results in the theory of four-dimensional manifolds" (in Russian), *Doklady Akademii Nauk, S. S. S. R.,* vol. 84 (1952), pp. 221-224.

[25] J-P. Serre, "Groupes d'homotopie et classes de groupes abéliens," *Annals of Mathematics,* vol. 58 (1953), pp. 258-294.

[25a] J. de Siebenthal, "Sur les sous-groupes fermés connexes des groupes de Lie clos," *Commentarii Mathematici Helvetici,* vol. 25 (1951), pp. 210-256.

[26] N. Steenrod, *Topology of fibre bundles,* Princeton Mathematical Series, no. 14, 1951.

[27] E. Stiefel, "Ueber eine Beziehung zwischen geschlossenen Lie'schen Gruppen und . . .", *Commentarii Mathematici Helvetici,* vol. 14 (1941-42), pp. 350-380.

[28] ———, "Kristallographische Bestimmung der Charaktere der geschlossenen Lie'-schen Gruppen," *ibid.,* vol. 17 (1944-45), pp. 165-200.

[29] R. Thom, "Quelques propriétés globales des variétés différentiables," *ibid.,* vol. 28 (1954), pp. 17-86.

[30] H. Toda, "Quelques tables des groupes d'homotopie des groupes de Lie," *Comptes Rendus des Séances de l'Académie des Sciences,* Paris, vol. 241 (1955), pp. 922-923.

[31] H. C. Wang, "Closed manifolds with homogeneous complex structure," *American Journal of Mathematics,* vol. 76 (1954), pp. 1-32.

[32] H. Weyl, "Theorie der Darstellung kontinuierlicher halb-einfacher Gruppen durch lineare Transformationen I, II, III," *Mathematische Zeitschrift,* vol. 23 (1925), pp. 271-309, vol. 24 (1926), pp. 328-395.

EXTENSIONS OF PURE STATES.*

By Richard V. Kadison [1] and I. M. Singer.

1. Introduction and preliminaries. The main concern of this paper is the problem of uniqueness of extensions of pure states from maximal abelian self-adjoint algebras of operators on a Hilbert space to the algebra of all bounded operators on that space. The answer, as many of us have suspected for several years, is in the negative. To the best of our knowledge, the problem is not recorded in the literature. We heard of it first from I. E. Segal and I. Kaplansky, though it is difficult to credit a problem which stems naturally from the physical interpretation and the inherent structure of a subject. This problem has arisen, in one form or another, in our work on several different occasions; and we have been gathering bits of information related to it, over the years. (The present solution is prompted by just such a reappearance.)

To state the problem precisely, let $\mathfrak{H}$ be a (complex) Hilbert space and $\mathfrak{A}$ an algebra of bounded operators invariant under the adjoint operation ($A \rightarrow A^*$), containing the identity operator, I, and closed in the uniform (operator bound) topology. The algebra, $\mathfrak{A}$, is a C^*-algebra, and a linear functional, f, on $\mathfrak{A}$ which is 1 at I and real, non-negative on positive operators (those operators, A, such that $(Ax, x) \geqq 0$ for each x in $\mathfrak{H}$), is a state of $\mathfrak{A}$. The set of states of $\mathfrak{A}$ is a convex subset of the dual of $\mathfrak{A}$ and is compact in the w^*-topology on the dual (the weak topology induced by $\mathfrak{A}$). The Krein-Milman theorem tells us that the set of states is the closed convex hull of its extreme points—these are the pure states of $\mathfrak{A}$. An argument of the Hahn-Banach type enables us to extend states from a C^*-subalgebra of $\mathfrak{A}$ to $\mathfrak{A}$ [4]. The set of extensions of such a state forms a compact convex subset of the dual whose extreme points can easily be shown to be pure states of $\mathfrak{A}$ [4], provided that the state of the subalgebra is pure. Thus, if a pure state has a unique pure state extension from a C^*-subalgebra of a C^*-algebra to the algebra, then the closed convex hull of this extension, viz.

* Received July 17, 1958.

[1] Alfred P. Sloan Fellow.

itself, is the set of all state extensions of the given pure state. Thus a pure state of a C^*-subalgebra has a unique state extension to the algebra if and only if it has a unique pure state extension.

If the C^*-algebra $\mathfrak{A}$ is abelian, the set of pure states is compact, and the natural mapping of $\mathfrak{A}$ into the second dual, followed by the restriction mapping to the set of pure states, is an algebraic, isometric, order isomorphism of $\mathfrak{A}$ onto the algebra of continuous, complex-valued functions on this compact space (the pure state space). (This isomorphism carries the adjoint operation in $\mathfrak{A}$ into complex conjugation in the function space.) An easy Zorn's lemma argument shows that $\mathfrak{A}$ is contained in a maximal abelian, self-adjoint subalgebra, $\mathcal{A}$, of the algebra, $\mathcal{B}$, of all bounded operators on $\mathcal{H}$. (Making use of the decomposition of operators as a sum of a self-adjoint and a skew-adjoint operator, it is not difficult to show that $\mathcal{A}$ is maximal with respect to the property of being abelian.) The fact that bounded families of operators in $\mathcal{A}$ have least upper bounds causes the pure state space of $\mathcal{B}$ to be extremely disconnected (i.e., the closure of each open set is open [8]). Examples of maximal abelian, self-adjoint algebras arise from the multiplication algebras on $L_2(X,\mu)$, with μ a measure on the space X, i.e. the algebra of operators T_g, with g an essentially bounded, μ-measurable function on X, where $T_g(h) = gh$, for each h in $L_2(X,\mu)$. In particular, with X the unit interval and μ Lebesgue measure on X, the algebra, $\mathcal{A}_c$, which arises will be referred to as 'the continuous maximal abelian algebra'; and with X, the integers, and $\mu(n) = 1$, for all n, the algebra, $\mathcal{A}_d$, which arises will be referred to as 'the discrete algebra.' (The maximal abelian algebras on finite-dimensional spaces are constructed as $\mathcal{A}_d$ is, with the integers replaced by a finite set. The algebra, $\mathcal{A}_d$, can also be viewed as the set of bounded diagonal matrices relative to a complete orthonormal basis.) Each maximal abelian algebra on a separable Hilbert space is unitarily equivalent to $\mathcal{A}_c$, $\mathcal{A}_d$, a finite-dimensional maximal abelian algebra, or the direct sum of $\mathcal{A}_c$ with one of the last two types. The problem of extensions of pure states from maximal abelian algebras to $\mathcal{B}$ (we consider mainly the separable case throughout this paper) reduces then, to a study of extensions from $\mathcal{A}_c$ and $\mathcal{A}_d$. Although we refer to $\mathcal{A}_d$ as 'the discrete maximal abelian algebra,' it should be noted that there is a great deal of 'non-discreteness' about it. In fact, its pure state space is easily identified with the β-compactification of the integers [9].

Each unit vector, x, gives rise to a state of $\mathcal{B}$ by means of the mapping, $A \rightarrow (Ax, x)$; and it is easily seen that this state, ω_x, is a pure state of $\mathcal{B}$. We refer to ω_x as a 'vector state' (also 'discrete state'). From our previous

remarks, we see that a pure state of an abelian C^*-algebra is multiplicative (the converse is true for all C^*-algebras), and from this, that a vector state is pure on an abelian C^*-algebra if and only if the vector which induces it is an eigenvector for each operator in the algebra. (Note that two vector states of $\mathcal{B}$ are equal if and only if the two vectors differ by a scalar multiple of modulus 1.) Since some operators in $\mathcal{A}_c$ have no eigenvectors, none of the pure states of $\mathcal{A}_c$ is a vector state—yet, each such pure state has a pure state extension to $\mathcal{B}$. Thus, there are pure states of $\mathcal{B}$ which are not vector states—we call these 'singular pure states.' Indeed, the points of the β-compactification of the integers which do not correspond to integers give rise to pure states of $\mathcal{A}_d$ which are not vector states and, therefore, have singular pure state extensions to $\mathcal{B}$. A well-known fact about singular pure states (which can be read out of the results of [3], for example) tells us that the singular pure states are precisely those which annihilate all completely continuous operators.

The uniqueness problem for extensions of pure states is the following: is there a unique state extension of a pure state of a maximal abelian self-adjoint algebra of the algebra, $\mathcal{B}$, of all bounded operators to $\mathcal{B}$? There are, of course, the two subdivisions of this problem—the question for $\mathcal{A}_d$ and the question for $\mathcal{A}_c$. It is quite easy to see that uniqueness of extension cannot be expected for abelian C^*-algebras other than the maximal abelian ones. In fact, if $\mathfrak{A}$ is an abelian C^*-algebra and $\mathcal{A}$ is a maximal abelian one containing it properly, then, making use of the function representation (of $\mathcal{A}$), the Stone-Weierstrass theorem assures us that $\mathfrak{A}$ does not separate pure states of $\mathcal{A}$, i.e., that there are two distinct pure states of $\mathcal{A}$ which agree on $\mathfrak{A}$ (and this restriction to $\mathfrak{A}$, being multiplicative, is pure). Naturally, one wonders why uniqueness should be expected in the maximal abelian case. Classically, our maximal abelian algebra, $\mathcal{A}$, would be that associated with an orthonormal basis, viz. $\mathcal{A}_d$, and the pure state, one due to a basis vector, x. Since the one-dimensional projections on the basis elements lie in $\mathcal{A}_d$, another pure state, ρ, which agrees with ω_x on $\mathcal{A}_d$ will annihilate all these projections with the exception of the one whose range contains x; so that if ρ is a vector state, that vector differs from x by a scalar multiple of modulus 1. Thus $\rho = \omega_x$, when we note that if ρ were not a vector state, it would annihilate all completely continuous operators and, in particular, all one-dimensional projections. More generally, if $\mathcal{A}$ is a maximal abelian algebra, ω_x is a pure state of $\mathcal{A}$, E is the one-dimensional projection whose range contains x, and ω is a pure state extension of ω_x from $\mathcal{A}$ to all bounded operators, then $\omega = \omega_x$.

In fact, x is an eigenvector for each operator in $\mathfrak{A}$, so that $\mathfrak{A}$ leaves the range of E invariant and, hence, commutes with E (since $\mathfrak{A}$ is a self-adjoint algebra). Thus E lies in $\mathfrak{A}$, and ω is a vector state ω_y, since $\omega(E) = \omega_x(E) = 1 \neq 0$. From $\omega_y(E) = \omega_x(E) = 1$, we conclude that $\| E \| = 1$ and that y lies in the range of E. Being a unit vector, y is a scalar multiple of modulus 1 of x, and $\omega_y = \omega_x$, on all bounded operators.

Having these results for vector pure states, it is not unreasonable to expect them to hold for arbitrary pure states in the same way that one passes from certain properties of the point spectrum to those of the general spectrum. Indeed, a casual handling of limit processes (just allowing oneself the minor luxury of a sequential limit in place of a directed limit) leads to a "proof" of the uniqueness of pure state extensions—false but provocative. Add to this evidence the elusiveness of a counter-example and one has the case for the conjecture.

In [5], von Neumann introduces a process for taking the "diagonal part" of certain operators in a von Neumann algebra (strongly closed C^*-algebra) relative to a maximal abelian self-adjoint subalgebra. Among other things, this process is linear, order preserving, and idempotent, and, so, provides a continuous way of simultaneously extending all the pure states of a maximal abelian algebra (provides a cross-section in the sheaf-like structure of state extensions over the pure state space of the maximal abelian algebra, so to speak). Two distinct diagonal processes will, of course, settle the pure state extension problem negatively for a particular maximal abelian algebra. In Section 2, we give a discussion of diagonal processes suitable for our applications, and in 3, we prove the uniqueness of diagonal processes for $\mathfrak{A}_d$ and the non-uniqueness of diagonal processes for $\mathfrak{A}_c$. The non-uniqueness proof is a mixture of abstract and classical techniques which produces a specific operator with distinct "diagonal parts" relative to $\mathfrak{A}_c$ (and, so, to which some pure state of $\mathfrak{A}_c$ can be extended in more than one way). In the last section, we discuss related questions concerning pure states.

2. Diagonal processes. The lemma which follows provides the means for constructing diagonal processes relative to maximal abelian algebras.

LEMMA 1. *If $\mathfrak{A}$ is an abelian von Neumann algebra generated by the projections $\{E\}_{n \in \mathcal{S}}$, $\mathcal{S}$ the set of positive integers, and p is a point of $\beta(\mathcal{S}) - \mathcal{S}$, where $\beta(\mathcal{S})$ is the β-compactification of $\mathcal{S}$, then there is a linear operator, $\mathfrak{D}_p$, whose domain is the set of bounded operators and which is such that:*

(a) *$\mathcal{D}_p(B)$ commutes with each E_n (so, lies in $\mathcal{A}'$, the commutant of $\mathcal{A}$), and $\mathcal{D}_p(B)$ is a weak closure point of operators $\{B^{|E_1|E_2|\cdots|E_n}\}$, where $T^{|E}$ is $ETE+(I-E)T(I-E)$.*

(b) *$\mathcal{D}_p(AB)=A\mathcal{D}_p(B)$, for each A in $\mathcal{A}$ (and $\mathcal{D}_p(BA)=\mathcal{D}_p(B)A)$.*

(c) *$\mathcal{D}_p(I)=I$, and $\mathcal{D}_p(B)\geqq 0$ if $B\geqq 0$.*

Proof. Note that

$$\|B^{|E}\|=\|EBE+(I-E)B(I-E)\|$$
$$=\max\{\|EBE\|,\|(I-E)B(I-E)\|\}\leqq\|B\|,$$

so that the function, f, defined on $\mathcal{S}$ by $f(n)=B^{|E_1|\cdots|E_n}$ maps $\mathcal{S}$ into the (weakly compact) ball of radius $\|B\|$ about 0 in the set of bounded operators. Note also that $B^{|E|F}=B^{|F|E}$ when $EF=FE$ and that $E(B^{|E})=(B^{|E})E$; so that $f(n)$ commutes with $E_1,\cdots,E_n$. From the properties of $\beta(\mathcal{S})$, we have that f has a unique extension, f_1, from $\mathcal{S}$ to $\beta(\mathcal{S})$ which is continuous and whose range is contained in the ball of radius $\|B\|$ about 0. We define $\mathcal{D}_p(B)$ to be $f_1(p)$. The observation that $(\alpha B+C)^{|E}=\alpha(B^{|E})+C^{|E}$, together with the fact that $\mathcal{S}$ is dense in the Hausdorff space $\beta(\mathcal{S})$, yields the linearity of $\mathcal{D}_p$ and the fact that $\mathcal{D}_p(B)$ is a weak closure point of $\{B^{|E_1|\cdots|E_n}\}$. If B is I, then $B^{|E_1|\cdots|E_n}=I$, for all n, so that $\mathcal{D}_p(B)=I$; and if $B\geqq 0$, then $B^{|E_1|\cdots|E_n}\geqq 0$, for all n, whence each weak closure point of $\{B^{|E_1|\cdots|E_n}\}$ is positive and, in particular, $\mathcal{D}_p(B)\geqq 0$. Moreover, $(AB)^{|E_k}=A(B^{|E_k})$ (and $(BA)^{|E_k}=(B^{|E_k})A$), with A in $\mathcal{A}$, so that $\mathcal{D}_p(AB)=A\mathcal{D}_p(B)$ (and $\mathcal{D}_p(BA)=\mathcal{D}_p(B)A$) (recall that left and right multiplication by A is weakly continuous). For a given n_0, $\mathcal{D}_p(B)$ is a weak closure point of $B^{|E_1|\cdots|E_m}$, with $m\geqq n_0$, each of which commutes with E_{n_0}. Thus $\mathcal{D}_p(B)$ commutes with E_{n_0}, for each n_0; so that $\mathcal{D}_p(B)$ lies in $\mathcal{A}'$.

DEFINITION 1. *A linear order preserving mapping from all bounded operators into the commutant of an abelian von Neumann algebra, $\mathcal{A}$, which is the identity on $\mathcal{A}$ is a "diagonal process relative to $\mathcal{A}$." If the image of each operator, B, is a weak closure point of operators $B^{|E_1|\cdots|E_n}$, with $E_1,\cdots,E_n$ in $\mathcal{A}$, the diagonal process is "proper"; otherwise, it is "improper."*

Remark 1. If $\mathcal{D}$ is proper and $B\in\mathcal{A}'$, $\mathcal{D}(B)$ is a weak closure point of $B^{|E_1|\cdots|E_n}=B$, so that $\mathcal{D}(B)=B$.

LEMMA 2. *If $\mathcal{D}$ is a diagonal process relative to $\mathcal{A}$ then $\mathcal{D}(AB)$*

$= A\mathcal{D}(B)$ *(and* $\mathcal{D}(BA) = \mathcal{D}(B)A$*) for each* A *in* $\mathfrak{A}$ *and each bounded operator,* B. *If* $\mathcal{D}$ *is weakly continuous on the unit ball, then it is the unique proper diagonal process relative to* $\mathfrak{A}$, *and* $\mathcal{D}(B)$ *is the weak limit of* $\{B_n\}$, *where* $B_n = B^{|E_1|\cdots|E_n}$ *and* $\{E_n\}$ *is a generating family of projections for* $\mathfrak{A}$.

Proof. We remark first, that if T and S are distinct operators in $\mathfrak{A}'$, there is an extension to $\mathfrak{A}'$ of some pure state of $\mathfrak{A}$ (in fact, a pure state extension) which differs on T and S. In fact, for each cardinal, n, there is a projection P_n in $\mathfrak{A}$ such that $\mathfrak{A}P_n$ is an n-fold copy of some maximal abelian algebra, $\mathfrak{A}_n$, acting on a Hilbert space, $\mathcal{H}_n$ (i.e. $\mathfrak{A}'P_n$ acting on $P_n(\mathcal{H})$ is unitarily equivalent to the algebra of $n \times n$ matrices with entries in $\mathfrak{A}_n$ acting on the direct sum of $\mathcal{H}_n$ with itself n times, in the usual way), and $\sum_n P_n = I$. With T and S distinct, $TP_n \neq SP_n$, for some n. If we can establish our result for $\mathfrak{A}P_n$ and its commutant $\mathfrak{A}'P_n$ (on $P_n(\mathcal{H})$), there is a pure state ρ_n of $\mathfrak{A}P_n$ and a state extension, ρ_n', of it to $\mathfrak{A}'P_n$ such that $\rho_n'(TP_n) \neq \rho_n'(SP_n)$. Defining ρ and ρ' by $\rho(A) = \rho_n(AP_n)$ and $\rho'(A') = \rho_n'(A'P_n)$, respectively, we note that ρ, being multiplicative, is a pure state of $\mathfrak{A}$, ρ' is a state extension of it and $\rho'(T) \neq \rho'(S)$. We may assume therefore that $\mathfrak{A}$ is an n-fold copy of the maximal abelian algebra $\mathfrak{A}_0$ acting on $\mathcal{H}_0$; from which $\mathfrak{A}'$ is the algebra of all $n \times n$ matrices, with entries in $\mathfrak{A}_0$, which give bounded operators acting upon the direct sum of $\mathcal{H}_0$ with itself n times. Let X be the pure state space of $\mathfrak{A}_0$, so that $\mathfrak{A}_0$ is algebraically isomorphic to the algebra, $C(X)$, of complex-valued continuous functions on X. Some entry in the matrix representations of T and S are distinct and, so, differ at a pure state ρ_0 of $\mathfrak{A}_0$. Let $\bar{\rho}_0(A')$ be the matrix obtained by replacing each entry of A' by its value at ρ_0, for A' in $\mathfrak{A}'$. The operator corresponding to this matrix is bounded and positive if A' is positive. Indeed, with n finite, the boundedness is automatic and the positivity then follows from the fact that $\bar{\rho}_0$ is adjoint-preserving and multiplicative, since ρ_0 is. (Boundedness and positivity can also be established when ρ_0 is not assumed pure by making use of [1].) Thus $\| \bar{\rho}_0(A') \| \leqq \| A' \|$, when n is finite. Applying this to the infinite case, we see that each finite minor has norm not exceeding $\| A' \|$, and again $\| \bar{\rho}_0(A') \| \leqq \| A' \|$. As in the finite case, it now follows that $\bar{\rho}_0(A')$ is positive if A' is. Since $\bar{\rho}_0(T) \neq \bar{\rho}_0(S)$, there is a unit vector, x_0, in the Hilbert space direct sum of the complex numbers with itself n times such that $(\bar{\rho}_0(T)x_0, x_0) \neq (\bar{\rho}_0(S)x_0, x_0)$. Now $\bar{\rho}_0(A)$ is a scalar multiple of I, for each A in $\mathfrak{A}$ so that $A \rightarrow (\bar{\rho}_0(A)x_0, x_0)$ is a pure state, ρ, of $\mathfrak{A}$ and $A' \rightarrow (\bar{\rho}_0(A')x_0, x_0)$ is an extension, ρ', of it to $\mathfrak{A}'$. By construction,

$\rho'(T) \neq \rho'(S)$. (The set of all state extensions of ρ to $\mathcal{A}'$ is a compact convex subset of the set of states of $\mathcal{A}'$ whose extreme points are pure states of $\mathcal{A}'$. If T and S coincide on each of these pure state extensions of ρ, they coincide on their finite convex combinations, so, on their (w^*-) closed convex hull, i. e., on all state extensions of ρ—in particular, on ρ'. Thus T and S differ on some pure state extension to $\mathcal{A}'$ of a pure state of $\mathcal{A}$.)

If ρ is a pure state of $\mathcal{A}$ and ρ' a state extension of ρ to all bounded operators, then $\rho'(AB) = \rho'(A)\rho'(B)$ (and $\rho'(BA) = \rho'(B)\rho'(A)$), for each A in $\mathcal{A}$. In fact, if E is a projection in $\mathcal{A}$, $\rho'(E) = 0$ or 1, since ρ' is multiplicative on $\mathcal{A}$. Thus $\rho'(EB)$ or $\rho'[(I-E)B]$ is 0 (as $\rho'(E)$ is 0 or 1, respectively), by an application of Schwarz's inequality to the inner product K, $H \rightarrow \rho'(H^*K)$ on the algebra of bounded operators. In either case, $\rho'(EB) = \rho'(E)\rho'(B)$. Thus $\rho'(AB) = \rho'(A)\rho'(B)$ for operators A in $\mathcal{A}$ which are linear combinations of projections in $\mathcal{A}$, and, by continuity of ρ' in the uniform topology, for uniform limits of such operators. From the spectral theorem, each self-adjoint operator in $\mathcal{A}$ is such a limit, so that $\rho'(AB) = \rho'(A)\rho'(B)$, for each A in $\mathcal{A}$ and each bounded operator, B.

In particular, if ρ'' is a state extension of ρ to $\mathcal{A}'$ and $\rho' = \rho'' \circ \mathfrak{D}$, then ρ' is a state extension of ρ to all bounded operators. (Recall that $\mathfrak{D}$ is the identity transform on $\mathcal{A}$.) Thus,

$$\begin{aligned}\rho''(\mathfrak{D}(AB)) &= \rho'(AB) = \rho'(A)\rho'(B) = \rho'(A)\rho''(\mathfrak{D}(B)) \\ &= \rho''(A)\rho''(\mathfrak{D}(B)) = \rho''(A\mathfrak{D}(B)),\end{aligned}$$

with A in $\mathcal{A}$ and B a bounded operator. (Note that the last equality follows from the considerations of the preceding paragraph applied to an extension of ρ'' from $\mathcal{A}'$—and hence of ρ from $\mathcal{A}$—to all bounded operators.) Since $\mathfrak{D}(AB)$ and $A\mathfrak{D}(B)$ are in $\mathcal{A}'$ and ρ'' is an arbitrary state extension to $\mathcal{A}'$ of an arbitrary pure state of $\mathcal{A}$, $\mathfrak{D}(AB) = A\mathfrak{D}(B)$, from the results of the first paragraph of this proof.

Suppose, now, that $\mathfrak{D}$ is weakly continuous on the unit ball (and, so, on each bounded ball), and that $\mathfrak{D}'$ is a proper diagonal process relative to $\mathcal{A}$. In this case, $\mathfrak{D}'(B)$ is a weak closure point of $\{B^{|E_1|\cdots|E_n}\}$. Each such weak closure point, A', is such that $\mathfrak{D}(A')$ is a weak closure point of $\{\mathfrak{D}(B^{|E_1|\cdots|E_n})\} = \{\mathfrak{D}(B)\}$, whence $\mathfrak{D}(A') = \mathfrak{D}(B)$. With A' in $\mathcal{A}'$, $\mathfrak{D}(A') = A'$, since $\mathfrak{D}$ is proper (cf. Remark 1). Thus $\mathfrak{D}'(B) = \mathfrak{D}(B)$ and $\mathfrak{D}' = \mathfrak{D}$. Moreover, each weak limiting point, A', of the sequence $(B^{|E_1|\cdots|E_n})$, lies in $\mathcal{A}'$, since it commutes with each E_n, and is a weak closure point of $\{B^{|E_1|\cdots|E_n}\}$, so that $A' = \mathfrak{D}(B)$. Since $\{B^{|E_1|\cdots|E_n}\}$ is

contained in the weakly compact ball of radius $\| B \|$ about 0, $(B^{|E_1|\cdots|E_n})$ has a weak limiting point which must be $\mathcal{D}(B)$. Thus $\mathcal{D}(B)$ is the weak limit of $(B^{|E_1|\cdots|E_n})$.

The next lemma notes the possibility of extending a positive linear mapping from a linear space of bounded operators containing I into an abelian von Neumann algebra to such mappings of all bounded operators into the abelian von Neumann algebra. The proof is a direct copy of the proof of Krein's extension theorem for states [4] making use of the boundedly complete lattice properties of abelian von Neumann algebras.

LEMMA 3. *If $\mathfrak{A}$ is an abelian von Neumann algebra, $\mathfrak{L}_0$ a self-adjoint linear space of bounded operators containing I, and ϕ_0 an adjoint-preserving, positive, linear mapping of $\mathfrak{L}_0$ into $\mathfrak{A}$, then ϕ_0 has an adjoint-preserving, positive linear extension with range in $\mathfrak{A}$ to the algebra, $\mathfrak{B}$, of all bounded operators.*

Proof. Partially order the set of adjoint-preserving, positive, linear mappings with range in $\mathfrak{A}$, domain a self-adjoint linear subspace of $\mathfrak{B}$ containing $\mathfrak{L}_0$, and which extend ϕ_0, by "function extension". Zorn's lemma applies, and there exists a maximal element, ϕ, with domain $\mathfrak{L}$. If $\mathfrak{L} \neq \mathfrak{B}$, there is a self-adjoint operator B not in $\mathfrak{L}$. Choose a positive integer n, such that $nI \geqq B \geqq -nI$. Then $-n\phi(I)$ is a lower bound for the subset $\{\phi(A) : A \in \mathfrak{L} \text{ and } A \geqq B\}$ of $\mathfrak{A}$ and $n\phi(I)$ is an upper bound for $\{\phi(C) : C \in \mathfrak{L} \text{ and } C \leqq B\}$. These subsets have a greatest lower bound, A_1, and least upper bound, A_0, respectively, in $\mathfrak{A}$, since $\mathfrak{A}$ is a boundedly complete lattice. Since $\phi(A) \geqq \phi(C)$, when $A \geqq B \geqq C$, with A and C in $\mathfrak{L}$, $A_1 \geqq A_0$. Choose A in $\mathfrak{A}$ such that $A_1 \geqq A \geqq A_0$, and define ϕ' on the linear space generated by B and $\mathfrak{L}$ as follows: $\phi'(\alpha B + C) = \alpha A + \phi(C)$, with C in $\mathfrak{L}$. Then ϕ' is an adjoint-preserving linear mapping with range in $\mathfrak{A}$ and is an extension of ϕ. If $\alpha B + C \geqq 0$, making use of the choice of A in each of the cases, $\alpha = 0$, $\alpha > 0$, $\alpha < 0$, we conclude that ϕ' is a positive mapping. Since $B \notin \mathfrak{L}$, the existence of ϕ' contradicts the maximality of ϕ. Thus $\mathfrak{L} = \mathfrak{B}$ and ϕ is an adjoint-preserving, positive, linear extension from $\mathfrak{L}$ to $\mathfrak{B}$ of ϕ_0.

Remark 2. With the notation of the preceding lemma, ϕ_0 has a unique positive extension from $\mathfrak{L}_0$ to $\mathfrak{B}$ if and only if the greatest lower bound of $\{\phi_0(A) : A \text{ in } \mathfrak{L}_0 \text{ and } A \geqq B\}$ is equal to the least upper bound of $\{\phi_0(C) : C \text{ in } \mathfrak{L}_0 \text{ and } B \geqq C\}$, for each self-adjoint operator, B, in $\mathfrak{B}$. In fact, if they are equal, the positivity condition forces each positive extension of ϕ_0 to take this value at B; and if they are not equal for some self-adjoint B, we may

extend ϕ_0 to the space generated by B and $\mathfrak{L}_0$ by assigning either of these values to B, and then extend the resulting mappings to two distinct positive mappings of $\mathcal{B}$ into $\mathcal{A}$, each of which extends ϕ_0.

Remark 3. If we take $\mathcal{A}$ as $\mathfrak{L}_0$ and ϕ_0 as the identity mapping on $\mathcal{A}$, the extension lemma guarantees the existence of a diagonal process with range in $\mathcal{A}$, and this diagonal process is improper if $\mathcal{A}$ is not maximal abelian (for a proper process is the identity on $\mathcal{A}'$, the commutant of $\mathcal{A}$). In case $\mathcal{A}$ is maximal abelian, and we proceed as just noted, the extension lemma and the the preceding remark provide another criterion for uniqueness of the diagonal process.

LEMMA 4. *If $\mathcal{D}$ is a diagonal process relative to the maximal abelian algebra $\mathcal{A}$, there is a *-representation, ϕ, of the algebra, $\mathcal{B}$, of all bounded operators which is an isomorphism on $\mathcal{A}$, and a projection E on the representation space such that*

$$\mathcal{D}(B) = \phi^{-1}[E(\phi(B))E]$$

for each B in $\mathcal{B}$.

Proof. Let $\{F_\alpha\}$ be a maximal orthogonal family of countably decomposable projections in $\mathcal{A}$, so that $\sum_\alpha F_\alpha = I$. Note that $\mathcal{D}_\alpha$, defined by $\mathcal{D}_\alpha(B) = \mathcal{D}(B)F_\alpha$, for B in the algebra, $\mathcal{B}_\alpha$, of bounded operators on $F_\alpha(\mathcal{H})$ ($\mathcal{H}$ the underlying Hilbert space of $\mathcal{B}$), is a diagonal process relative to the maximal abelian algebra $\mathcal{A}F_\alpha$ (on $F_\alpha(\mathcal{H})$). If we can find a representation ϕ_α of $\mathcal{B}_\alpha$ and a projection E_α with the properties described in the lemma (relative to $\mathcal{A}_\alpha$), then the direct sum, ϕ, of the representations and E, the sum of E_α, establish the result for $\mathcal{D}$.

We may assume that $\mathcal{A}$ is countably decomposable, so that there exists a (unit) separating vector, x, for $\mathcal{A}$. We define a state, ρ, of $\mathcal{B}$ by: $\rho(B) = \omega_x(\mathcal{D}(B))$. From Gelfand-Neumark [1] and Segal [6], ρ gives rise to a *-representation ϕ of $\mathcal{B}$ constructed as follows. The set of operators B in $\mathcal{B}$ such that $\rho(B^*B) = 0$ is a left ideal, $\mathcal{J}$. The quotient vector space $\mathcal{B}/\mathcal{J}$ has a positive definite inner product on it defined by

$$[B + \mathcal{J}, C + \mathcal{J}] = \rho(C^*B),$$

so that the completion, $\mathcal{H}_0$, of $\mathcal{B}/\mathcal{J}$ relative to this inner product is a Hilbert space. The mapping, $B + \mathcal{J} \to AB + \mathcal{J}$, on $\mathcal{B}/\mathcal{J}$ to $\mathcal{B}/\mathcal{J}$ extends to a bounded operator $\phi(A)$, for each A in $\mathcal{B}$ and ϕ is the *-representation in question. That ϕ is an isomorphism on $\mathcal{A}$ (with range $\mathfrak{A}_0$, let us say) is a

consequence of the definition of ρ. In fact, if $\phi(A)=0$, then

$$0=[A+\mathfrak{J},A+\mathfrak{J}]=\rho(A^*A)=\omega_x(\mathcal{D}(A^*A))=\|Ax\|^2,$$

for A in $\mathcal{A}$, whence $A=0$. (Recall that x was chosen as a separating vector for $\mathcal{A}$.)

Let E be the projection on the closure of $\{A+\mathfrak{J}:A\in\mathcal{A}\}$. Our final assertion is that $\phi[\mathcal{D}(B)]=E\phi(B)E$, both operators restricted to $E(\mathcal{H}_0)$. We have

$$\begin{aligned}[\phi[\mathcal{D}(B)](A+\mathfrak{J}),C+\mathfrak{J}]&=\rho(C^*\mathcal{D}(B)A)\\&=\omega_x[C^*\mathcal{D}(B)A]=\omega_x[\mathcal{D}(C^*\mathcal{D}(B)A)]\end{aligned}$$

and

$$\begin{aligned}[E\phi(B)E(A+\mathfrak{J}),C+\mathfrak{J}]&=[\phi(B)(A+\mathfrak{J}),C+\mathfrak{J}]\\&=\rho(C^*BA)=\omega_x[\mathcal{D}(C^*BA)]=\omega_x[C^*\mathcal{D}(B)A],\end{aligned}$$

with C and A in $\mathcal{A}$. Thus, as operators on $E(\mathcal{H}_0)$, $\phi[\mathcal{D}(B)]=E\phi(B)E$.

Remark 4. Relative to the scalar algebra, $\{\lambda I\}$ the identity mapping on $\mathcal{B}$ is the unique proper diagonal process, and each state, ρ, of $\mathcal{B}$ yields an improper diagonal process by means of the mapping $B\to\rho(B)I$.

Remark 5. If $\mathcal{D}$ is a diagonal process relative to $\mathcal{A}_c$, then $\mathcal{D}(C)=0$ for each completely continuous operator, C. In fact, if ρ is a pure state of $\mathcal{A}_c$, $\rho\circ\mathcal{D}$ is a state extension of ρ from $\mathcal{A}_c$ to $\mathcal{B}$ and so, the finite convex combinations of pure state extensions, ρ', of ρ to $\mathcal{B}$ have $\rho\circ\mathcal{D}$ as a w^*-limit point. Now $\rho'(C)=0$ or else ρ' is a vector state, ω_x. But then ω_x is pure on $\mathcal{A}_c$, so that x is a simultaneous eigenvector for $\mathcal{A}_c$—a contradiction. Thus $\rho'(C)=0$, so that finite convex combinations of such ρ' annihilate C and $\rho\circ\mathcal{D}(C)=\rho[\mathcal{D}(C)]=0$. Hence $\mathcal{D}(C)=0$.

3. Uniqueness and non-uniqueness of diagonal processes. We consider $\mathcal{A}_d$ first and show that there is a unique diagonal process relative to it. Let $\{x_k\}$ be an orthonormal basis for $\mathcal{H}$, the Hilbert space upon which $\mathcal{A}_d$ acts, relative to which each operator in $\mathcal{A}_d$ is diagonal. Let us define $\mathcal{D}(B)$ for a bounded operator, B, to be the operator whose matrix representation relative to $\{x_k\}$ is the diagonal matrix with diagonal that of the matrix representation for B relative to $\{x_k\}$. Clearly, then, $\mathcal{D}$ is a diagonal process relative to $\mathcal{A}_d$. With $x=\sum_k\alpha_kx_k$ and $\|B\|\leqq 1$,

$$|(\mathcal{D}(B)x,x)|\leqq\sum|\alpha_k|^2|(\mathcal{D}(B)x_k,x_k)|=\sum|\alpha_k|^2|(Bx_k,x_k)|,$$

and for suitably large N, $\sum_{k \geqq N} |\alpha_k|^2 |(Bx_k, x_k)| < \epsilon/2$. Thus, with

$$|(Bx_k, x_k)| < \epsilon/2 \, \| x \|, \qquad k = 1, \cdots, N,$$

we have $|(\mathcal{D}(B)x, x)| \leqq \sum |\alpha_k|^2 |(Bx_k, x_k)| < \epsilon$, so that $\mathcal{D}$ is a continuous mapping at 0 on the unit ball of the algebra, $\mathcal{B}$, of all bounded operators in the weak operator topology into $\mathcal{B}$ in this topology. Since $\mathcal{B}$ is a topological linear space in the weak operator topoloygy and $\mathcal{D}$ is linear, $\mathcal{D}$ is continuous on the unit ball of $\mathcal{B}$ in this topology. From Lemma 2, it follows that $\mathcal{D}$ is the unique proper diagonal process relative to $\mathfrak{A}_d$. By other considerations, we show that $\mathcal{D}$ is the *unique diagonal process* relative to $\mathfrak{A}_d$.

THEOREM 1. *The unique diagonal process relative to* $\mathfrak{A}_d$ *is* $\mathcal{D}$.

Proof. If $\mathcal{D}'$ is a diagonal process distinct from $\mathcal{D}$, then $\mathcal{D}'(B) \neq \mathcal{D}(B)$ for some B in $\mathcal{B}$; so that $(\mathcal{D}'(B)x_k, x_k) \neq (\mathcal{D}(B)x_k, x_k)$, for some k—whence $\omega_{x_k} \circ \mathcal{D}' \neq \omega_{x_k} \circ \mathcal{D}$. But ω_{x_k} is a vector pure state of $\mathfrak{A}_d$ and has a unique state extension to $\mathcal{B}$. Thus $\mathcal{D}$ is the unique diagonal process relative to $\mathfrak{A}_d$.

Of course, this does not establish that the pure states of $\mathfrak{A}_d$ which are not vector states (the points of the β-compactification of the integers other than integer points) have unique state extensions to $\mathcal{B}$.

THEOREM 2. *There is more than one proper diagonal process relative to* $\mathfrak{A}_c$; *pure state extension is not unique relative to* $\mathfrak{A}_c$.

Proof. If we represent our Hilbert space, $\mathcal{H}$ as $L_2(0,1)$ under Lebesgue measure and $\mathfrak{A}_c$ as the multiplication algebra of this measure space, then the set of projections $\{E_{km} : m = 1, 2, \cdots, k = 1, \cdots, m\}$ corresponding to multiplication by the characteristic function of the closed intervals $[(k-1)/m, k/m]$ generate $\mathfrak{A}_c$. Now $I = \sum_{k=1}^{m} E_{km}$, so that $B^{|E_{1m}|\cdots|E_{mm}} = \sum_{k=1}^{m} E_{km}BE_{km}$, and $B^{|E_{1m}|\cdots|E_{mm}|E_{1mn}|\cdots|E_{mnmn}} = \sum_{k=1}^{mn} E_{kmn}BE_{kmn}$. From Lemma 2, if there is a unique diagonal process $\mathcal{D}$ of the form $\mathcal{D}_p$, p in the β-compactification of the integers but not an integer, in particular, if there is a unique proper diagonal process, then $\mathcal{D}(B)$ is the weak limit (with respect to j) of $\sum_{k=1}^{m} E_{km}BE_{km}$, where $m = 2^j$. In fact, if this is not the case for some B, then $\mathcal{D}_p(B) \neq \mathcal{D}_{p'}(B)$ for some points p and p' in $\beta(\mathcal{J}) - \mathcal{J}$. We shall exhibit such a B.

The functions, f_n, defined by $f_n(x) = e^{2\pi i n x}$, for $n = 0, \pm 1, \cdots$, form an orthonormal basis for $\mathcal{H}$. As B, we shall take the projection, G, on the subspace spanned by certain of these elements $\{f_{n_j} : j = 1, 2, \cdots\}$ (to be

specified later). We have

$$(E_{km}GE_{km}(1),1)=\sum_{j=1}^{\infty}|(f_{n_j},E_{km}(1))|^2=\sum_{j=1}^{\infty}\left|\int_{(k-1)/m}^{k/m}e^{2\pi i n_j x}\,dx\right|^2$$

$$=\sum_{j=1}^{\infty}|(1/2\pi i n_j)[e^{2\pi i n_j k/m}-e^{2\pi i n_j (k-1)/m}]|^2$$

$$=\sum_{j=1}^{\infty}(1/4\pi^2 n_j^2)|e^{2\pi i n_j/m}-1|^2,$$

whence

$$((\sum_{k=1}^{m}E_{km}GE_{km})(1),1)=\sum_{j=1}^{\infty}(m/4\pi^2 n_j^2)|e^{2\pi i n_j/m}-1|^2$$

$$=\sum_{j=1}^{\infty}(m/\pi^2 n_j^2)\sin^2(\pi n_j/m).$$

We show that, for a suitable choice of $n_1, n_2, \cdots$,

$$(m/\pi^2)\sum_{j=1}^{\infty}(1/n_j^2)\sin^2(\pi n_j/m) \tag{1}$$

does not tend to a limit as m $(=2^r)$ tends to ∞. For our set, $\{n_j\}$, choose all integers in the closed intervals $[2^{2^k-2}, 2^{2^k-1}]$, $k=1,2,\cdots$ (so that $n_1=1$, $n_2=2, n_3=4, n_4=5,\cdots$).

Note that (1) may be rewritten as

$$(1/\pi)\sum_{j=1}^{\infty}(\pi n_j/m)^{-2}[\sin^2(\pi n_j/m)](\pi/m)\ (=a_m)$$

which is the integral over $[0,\infty]$ of the step function, s_m, defined as $(\pi n_j/m)^{-2}[\sin^2(\pi n_j/m)]\cdot(1/\pi)$ on the interval $[\pi(n_j-1)/m, \pi n_j/m]$, $j=1,2,\cdots$, and 0 elsewhere, and that, with $m\equiv 0\ (4)$,

$$(1/\pi)\sum_{m/4<n_j\leqq m/2}(\pi n_j/m)^{-2}[\sin^2(\pi n_j/m)]\cdot(\pi/m)$$
$$=\int_{\pi/4}^{\pi/2}s_m(x)\,dx\ (=b_m).$$

Now, with $m_k=2^{2^k}$, s_{m_k} is a Riemann approximating step function to $\pi^{-1}x^{-2}\sin^2 x$, on the interval $[\pi/4,\pi/2]$. Thus, if a_{2^m} tends to a limit as m tends to ∞, so does a_{m_k} as k tends to ∞, and

$$\lim_m a_{2^m}=\lim_k a_{m_k}\geqq \lim_k b_{m_k}=\pi^{-1}\int_{\pi/4}^{\pi/2}x^{-2}\sin^2 x\,dx>\pi^{-2}.$$

(For the last inequality, note that the derivative, $2x^{-3}\sin x\ (x\cos x-\sin x)$, of $x^{-2}\sin^2 x$ is negative on $[\pi/4,\pi/2]$, so that $x^{-2}\sin^2 x>4\pi^{-2}$ on $[\pi/4,\pi/2]$.)

On the other hand, there are no terms n_j in $(2^{2^{k-1}}, 2^{2^{k+1}-2})$. Thus, with $r_k = 2^{2^{k+1}-2}$, s_{r_k} is 0 on $[\pi 2^{2^{k-1}}(2^{2^{k+1}-2})^{-1}, \pi k/(k+1)]$, whose left end point tends to 0 as k tends to ∞. Since each s_m is bounded (e.g. by 1) on $[0,\pi]$, we have $\lim_{k\to\infty}\int_0^\pi s_{r_k}(x)\,dx = 0$. Thus, if $\lim_m a_{2^m}$ exists, then

$$\pi^{-2} < \lim_k a_{m_k} = \lim_k a_{r_k} = \lim_k \int_0^\infty s_{r_k}(x)\,dx$$
$$= \lim_k \int_\pi^\infty s_{r_k}(x)\,dx \leqq \lim_k (1/\pi)\int_\pi^\infty x^{-2}\,dx = \pi^{-2},$$

a contradiction. (Note that $s_m(x) \leqq \pi^{-1}x^{-2}$, for x in $[0,\infty)$.) Thus $\lim_k a_{2^k}$ does not exist, and G does not have a unique diagonal part relative to $\mathcal{A}_c$ (G is the projection on the space spanned by $e^{2\pi i n_j x}$, where $\{n_j\}$ is as described). From our earlier discussion, there are pure states of $\mathcal{A}_c$ which do not have unique state (and pure state) extensions to all bounded operators (in fact, which have distinct values on G).

4. The pure states. We have noted that non-uniqueness of diagonal processes implies non-uniqueness of pure state extension and that uniqueness of the diagonal process does not lead to uniqueness of pure state extension. The problem of uniqueness of pure state extension (and even that of diagonal processes) may be raised in more refined form. Given a maximal abelian self-adjoint algebra $\mathcal{A}$: for which operators, B, is it the case that all extensions of the same pure state of $\mathcal{A}$ coincide on B?

LEMMA 5. *If $\mathcal{A}$ is a maximal abelian algebra then there exists a sequence of projections $\{E_n\}$ in $\mathcal{A}$ such that $B^{|E_1|\cdots|E_n}$ converges to an operator of $\mathcal{A}$ in the uniform topology if and only if $\rho_1(B) = \rho_2(B)$ for each pair of states, ρ_1, ρ_2, of all bounded operators such that $\rho_1 \mid \mathcal{A} = \rho_2 \mid \mathcal{A}$ is a pure state of $\mathcal{A}$.*

Proof. Suppose that a sequence such as $\{E_n\}$ exists, for the operator B. Then, with ρ_1 and ρ_2 states of all bounded operators whose restrictions to $\mathcal{A}$ are pure and equal, $\rho_1(B^{|E}) = \rho_1(B)$ and $\rho_2(B^{|E}) = \rho_2(B)$ for each projection, E, in $\mathcal{A}$. In fact, $\rho_1(E)$ is 0 or 1, since E is a projection in $\mathcal{A}$ and ρ_1 is pure on $\mathcal{A}$, while $\rho_1(B^{|E}) = \rho_1(E)\rho_1(B)\rho_1(E) + \rho_1(I-E)\rho_1(B)\rho_1(I-E) = \rho_1(B)$ (cf. Lemma 2, second paragraph of the proof). Thus,

$$\rho_1(B^{|E_1|\cdots|E_n}) = \rho_1(B) \text{ and } \lim \rho_1(B^{|E_1|\cdots|E_n}) = \rho_1(A) = \rho_1(B),$$

where $B^{|E_1|\cdots|E_n}$ tends uniformly to the operator A in $\mathcal{A}$ (recall that states of C^*-algebras are continuous in the uniform topology). Similary, $\rho_2(B) = \rho_2(A)$ $(= \rho_1(A) = \rho_1(B))$, so that $\rho_1(B) = \rho_2(B)$.

Suppose now that all extensions of each given pure state of $\mathfrak{A}$ coincide on B. Clearly then each diagonal process relative to $\mathfrak{A}$ has the same value, A, at B. We shall find $\{E_n\}$ such that $B^{|E_1|\cdots|E_n}$ tends uniformly to A, or equivalently, that $(B-A)^{|E_1|\cdots|E_n}=B^{|E_1|\cdots|E_n}-A$ tends uniformly to 0. Of course, extensions of a given pure state of $\mathfrak{A}$ coincide on $B-A$, and have value 0 (since $B-A$ has diagonal 0 under each diagonal process relative to $\mathfrak{A}$). We may assume, therefore, that each extension of a pure state of $\mathfrak{A}$ has value 0 on B, and that B is self adjoint.

Now $\mathfrak{A}$ is *-isomorphic with $C(X)$, where X is extremely disconnected—each point, x_0, of X corresponds to a pure state, ρ_{x_0}, of $\mathfrak{A}$ (and conversely). Since each state extension of ρ_{x_0} has the value 0 on B, we have

$$0=\inf\{\rho_{x_0}(A) : A \text{ in } \mathfrak{A}, A\geqq B\}=\sup\{\rho_{x_0}(A) : A \text{ in } \mathfrak{A}, B\geqq A\}.$$

Thus, we can choose operators A_{x_0} and A^{x_0} in $\mathfrak{A}$ such that $A^{x_0}\geqq B\geqq A_{x_0}$ and $1/n>\bar{A}^{x_0}(x_0)\geqq 0\geqq \bar{A}_{x_0}(x_0)>-1/n$, where $\bar{A}$ is the function in $C(X)$ corresponding to an operator, A, in $\mathfrak{A}$. It follows that there is a closed-open set, containing x_0, whose characteristic function corresponds to a projection E_{n,x_0} in $\mathfrak{A}$, on which $\bar{A}^{x_0}$ is less than $1/n$ and $\bar{A}_{x_0}$ is greater than $-1/n$. Then

$$\begin{aligned}(1/n)E_{n,x_0} &\geqq E_{n,x_0}A^{x_0}\\ &=E_{n,x_0}A^{x_0}E_{n,x_0}\geqq E_{n,x_0}BE_{n,x_0}\geqq E_{n,x_0}A_{x_0}\geqq(-1/n)E_{n,x_0},\end{aligned}$$

so that $\| E_{n,x_0}BE_{n,x_0}\|\leqq 1/n$. Since X is compact, the closed-open sets corresponding to E_{n,x_0}, for each x_0, cover X and have a finite subcovering. Denote the corresponding projections by $E_{n1},\cdots,E_{nk_n}$. We may replace this set of projections (using intersections and relative complements) by an orthogonal set of projections in $\mathfrak{A}$ each of which is contained in some E_{nj} and such that each E_{nj} is the sum of projections in the new finite set. If E is one of the new projections, contained, say, in E_{n1}, then

$$\| EBE\|=\| EE_{n1}BE_{n1}E\|\leqq\| E\|^2\| E_{n1}BE_n\|\leqq 1/n.$$

We may assume that $E_{n1},\cdots,E_{nk_n}$ are orthogonal, so that their sum is I (their corresponding closed-open sets cover X). Thus

$$\| B^{|E_{n1}|\cdots|E_{nk_n}}\|=\|\sum_{j=1}^{k_n}E_{nj}BE_{nj}\|\leqq 1/n.$$

The sequence $E_{11},E_{12},\cdots,E_{1k_1},E_{21},\cdots,E_{2k_2},\cdots$ will serve as the desired sequence, $\{E_n\}$.

Remark 6. If the state extensions to $\mathfrak{B}$ of a state of a maximal abelian

algebra, $\mathcal{A}$, coincide on each operator of a certain set, $\mathcal{S}$, (i.e. the restriction of these extensions to $\mathcal{S}$ defines a single-valued function on $\mathcal{S}$) then the same is true for the uniform closure of the self-adjoint linear space generated by $\mathcal{S}$ and for the set of those operators, T, for which there is a family $\{E_n\}$ of projections in $\mathcal{A}$ such that $T^{|E_1|\cdots|E_n}$ has a uniform limit in $\mathcal{S}$.

THEOREM 3. *All state extensions to* $\mathcal{B}$ *of a pure state of* $\mathcal{A}_d$ *coincide on each permutation matrix* (i.e. *each linear operator which permutes the eigenvectors of* $\mathcal{A}_d$).

Proof. Let $\{x_n\}_{n=1,2,\cdots}$ be a basis of eigenvectors for $\mathcal{A}_d$, and let $Tx_n = x_{\alpha(n)}$, where α is a permutation of $\mathcal{J}$. Then, the matrix of T relative to $\{x_n\}$ has 1 at each entry $\alpha(n), n$ and zeros at the other entries (it is a permutation matrix). Let $\mathcal{J}_1$ be the fixed points of α. We shall define three other sets of integers, $\mathcal{J}_2$, $\mathcal{J}_3$, and $\mathcal{J}_4$. Assign to $\mathcal{J}_2$ the first element of $\mathcal{J}$ not in $\mathcal{J}_1$ and suppose that each element of $\mathcal{J}$ less than n has been assigned to one of $\mathcal{J}_1, \cdots, \mathcal{J}_4$ in such a way that j and $\alpha(j)$ are not in the same set if they are distinct. Assign n to the first one of $\mathcal{J}_2$, $\mathcal{J}_3$, $\mathcal{J}_4$ which contains neither $\alpha(n)$ nor $\alpha^{-1}(n)$, unless $\alpha(n) = n$, in which case, assign n to $\mathcal{J}_1$. In this way, we construct four pairwise disjoint sets $\mathcal{J}_1$, $\mathcal{J}_2$, $\mathcal{J}_3$, $\mathcal{J}_4$ with union $\mathcal{J}$ such that $\alpha(n)$ and n lie in no one of them, unless they are equal (in which case it lies in $\mathcal{J}_1$). Let E_j, $j = 1, \cdots, 4$ be the projection (in $\mathcal{A}_d$) on the subspace spanned by $\{x_k : k \text{ in } \mathcal{J}_j\}$. From the construction, $E_1TE_1 = E_1$ and $E_jTE_j = 0$, $j = 2, 3, 4$, while $E_1, \cdots, E_4$ are mutually orthogonal and have sum I. Thus $T^{|E_1|E_2|E_3|E_4} = E_1$, which lies in $\mathcal{A}_d$. An application of Lemma 5 completes the proof.

Combining Theorem 3 with Remark 6, we see that pure state extension from $\mathcal{A}_d$ is unique to the algebra of linear combinations of permutation matrices (and to its uniform closure). We note that the proof of Theorem 3 applies to more general 0, 1 matrices (e.g. to those operators which annihilate some basis vectors and are one-one mappings of the others into the set of basis vectors).

5. Related questions. The results that we have obtained leave the question of uniqueness of extension of the singular pure states of $\mathcal{A}_d$ open. We incline to the view that such extension is non-unique (although the diagonal process is unique—Theorem 1, and there is a large class of operators to which extension is unique—Theorem 3). Our considerations also raise the question of whether or not each pure state of $\mathcal{B}$ is the extension of some pure state of some maximal abelian algebra. (This is true for the vector

states of $\mathfrak{B}$.) With regard to this last question, one can partially order the states of $\mathfrak{B}$ by comparing the sets of elements on which they give "definite information." (We say that the state, ω of $\mathfrak{B}$ is definite on a self-adjoint operator, A, when ω is pure on the C^*-algebra generated by A-equivalently, when $\omega(A^2) = \omega(A)^2$. The set of operators on which ω is definite is "the definite set" of ω.)

THEOREM 4. *A state of $\mathfrak{B}$ is pure if and only if its definite set is maximal (with respect to inclusion).*

Proof. If $\mathcal{K}$ is the left kernel of ω, then the definite set of ω is $\{\mathcal{K}_* + \lambda I\}$, where $\mathcal{K}_*$ is the set of self-adjoint operators in $\mathcal{K}$ and λ is a real number. (Note that the set of self-adjoint operators in a uniformly closed left ideal determines that ideal—in fact, the positive operators in the ideal determine it [7].) Indeed, if A is in $\mathcal{K}_*$, then $0 = \omega(A) = \omega(A)^2 = \omega(A^2)$ (by definition of $\mathcal{K}$), so that ω is definite on $\mathcal{K}_*$ and hence on $\{\mathcal{K}_* + \lambda I\}$. On the other hand, if ω is definite on B, then it is definite on $B - \omega(B)I$, so that $\omega([B - \omega(B)I]^2) = \omega(B - \omega(B)I)^2 = 0$ and $B - \omega(B)I$ is in $\mathcal{K}_*$, B is in $\{\mathcal{K}_* + \lambda I\}$. If $\mathcal{K}$ is not a maximal left ideal and $\mathcal{J}$ is a left ideal in $\mathfrak{B}$ containing $\mathcal{K}$ properly, choose A in $\mathcal{J}_*$ not in $\mathcal{K}$. If $A = B + \lambda I$, with B in $\mathcal{K}_*$, then $A - B = \lambda I$ is in $\mathcal{J}$, so that $\lambda = 0$, $A = B$ is in $\mathcal{K}$—a contradiction. Thus $\{\mathcal{J}_* + \lambda I\}$ contains $\{\mathcal{K}_* + \lambda I\}$ properly. It follows that the definite set of ω is maximal only if its left kernel is a maximal left ideal—which implies that ω is pure [2].

Suppose, now, that $\mathcal{K}$ is a maximal left ideal and that $\mathcal{J}$ is a left ideal such that $\{\mathcal{J}_* + \lambda I\}$ contains $\{\mathcal{K}_* + \lambda I\}$, the definite set of some pure state. We show that $\{\mathcal{J}_* + \lambda I\}$, the definite set of an arbitrary state, coincides with $\{\mathcal{K}_* + \lambda I\}$, in this case. Passing to a maximal left ideal containing $\mathcal{J}$, we may assume that $\mathcal{J}$ itself is maximal; so that $\mathcal{J}$ is the left kernel of a pure state, ρ, of $\mathfrak{B}$. If $\mathcal{J}$ annihilates a vector, y, then so must $\mathcal{K}$; for otherwise, $\mathcal{K}_*$ contains all self-adjoint completely continuous operators, and in particular, one which maps y onto a non-zero vector orthogonal to y-contradicting the fact that $\{\mathcal{J}_* + \lambda I\}$ has y as an eigenvector and contains $\{\mathcal{K}_* + \lambda I\}$. Thus $\mathcal{K}_*$ consists of all self-adjoint operators annihilating some vector, z, and has y as an eigenvector; so that z is a scalar multiple of y, $\mathcal{K}_*$ annihilates y, $\mathcal{K} = \mathcal{J}$, and $\{\mathcal{K}_* + \lambda I\} = \{\mathcal{J}_* + \lambda I\}$.

We may assume that $\mathcal{J}$ does not annihilate a vector and, so, contains $\mathcal{C}$, the ideal of completely continuous operators in $\mathfrak{B}$. Thus, ϕ, the irreducible representation of $\mathfrak{B}$ associated with ρ has $\mathcal{C}$ as kernel. If A is in $\mathcal{K}_*$ but not in $\mathcal{J}_*$, then $\rho(A^2) = \rho(A)^2 \neq 0$; so that $\rho(E) \neq 0$ for some spectral

projection, E, of A corresponding to an interval whose closure does not contain 0. In fact, from the Spectral Theorem, A is a uniform limit of finite linear combinations of such spectral projections, and if ρ annihilates each of them, then since ρ is uniformly continuous, $\rho(A)=0$. Since E corresponds to an interval whose closure does not contain 0, $I-E+AE$ has an inverse, B; so that $BEA=E[B(I-E+AE)]=E$ is in $\mathcal{K}_*$ and hence in $\{\mathcal{J}_*+\lambda I\}$. Moreover, ECE is in $\mathcal{K}_*$, hence in $\{\mathcal{J}_*+\lambda I\}$, for each self-adjoint C in $\mathcal{B}$. Now ϕ maps $\{\mathcal{J}_*+\lambda I\}$ into the set of self-adjoint operators which have x as an eigenvector, where x is a vector such that $\omega_x\phi=\rho$; so that the projection, $\phi(E)$, has x in its range (since $\rho(E)\neq 0$), and $\phi(E)\phi(C)\phi(E)x=\phi(E)\phi(C)x=ax$. Since ϕ is an irreducible representation of $\mathcal{B}$, $\phi(E)$ must be the one-dimensional projection whose range contains x. But ρ annihilates $\mathcal{C}$, and $\rho(E)\neq 0$. Thus E is infinite dimensional, and $E=F+I-F$, where F and $I-F$ are infinite dimensional; so that $\phi(E)=\phi(F)+\phi(I-F)$, with $\phi(F)$ and $\phi(I-F)$ non-zero orthogonal projections. (Recall that the kernel of ϕ is $\mathcal{C}$). Hence $\phi(E)$ cannot be one-dimensional, each A in $\mathcal{K}_*$ lies in $\mathcal{J}_*$, $\mathcal{K}$ is contained in $\mathcal{J}$ and $\mathcal{K}=\mathcal{J}$, by maximality, and $\{\mathcal{K}_*+\lambda I\}$ is a maximal definite set.

Presumably, the definite set of each pure state contains the set of self-adjoint elements of some (perhaps many) maximal abelian algebras. A general question of obvious interest is that of the classification of the irreducible representations of $\mathcal{B}$. We know from [3] that the separable ones are all unitarily equivalent (to the algebra of bounded operators on separable Hilbert space) and are associated with vector states. The vector states of $\mathcal{B}$ are unitarily equivalent. Is this the case for the singular pure states of $\mathcal{B}$? A clever counting argument of Kaplansky's shows that this is not so. In fact, each pure state of $\mathcal{A}_d$ has a pure state extension to $\mathcal{B}$, so that there are at least 2^C pure states of $\mathcal{B}$ (the pure state space of $\mathcal{A}_d$ is $\beta(\mathcal{S})$ which has cardinality 2^C), while there are only C operators (as can easily be seen from the matrix representation relative to a countable orthonormal basis.) Each unitary equivalence class contains at most C states, so that there are 2^C inequivalent singular pure states.

COLUMBIA UNIVERSITY
AND
MASSACHUSETTS INSTITUTE OF TECHNOLOGY.

REFERENCES.

[1] I. Gelfand and M. Neumark, "On the imbedding of normed rings into the ring of operators in Hilbert space," *Recueil Mathématique (Matematičeskiĭ Sbornik)* Nosia Seria, vol. 12 (1943), pp. 197-213.

[2] R. Kadison, "Irreducible operator algebras," *Proceedings of the National Accdemy of Sciences (U. S. A.)*, vol. 43 (1957), pp. 273-276.

[3] I. Kaplansky, "Representations of separable operator algebras," *Duke Mathematical Journal,* vol. 19 (1952), pp. 219-222.

[4] M. Krein, "Sur les fonctionnelles positives additives dans les espaces linéaires normés," *Communications de l'Institut des Sciences Mathématique et Mécanique de Kharkoff,* série 4, t. XIV (1937).

[5] J. von Neumann, "On rings of operators, III," *Annals of Mathematics,* vol. 41 (1940), pp. 94-161.

[6] I. Segal, "Irreducible representations of operator algebras," *Bulletin of the American Mathematical Society,* vol. 53 (1947), pp. 73-88.

[7] ———, "Two-sided ideals in operator alegbras," *Annals of Mathematics,* vol. 50 (1949), pp. 856-865.

[8] M. Stone, "Boundedness in function-lattices," *Canadian Journal of Mathematics,* vol. 1 (1949), pp. 176-186.

[9] ———, "Applications of the theory of Boolean rings to general topology," *Transactions of the American Mathematical Society,* vol. 41 (1937), pp. 375-481.

A GENERAL THEORY OF ALGEBRAIC GEOMETRY OVER DEDEKIND DOMAINS, III.*

Absolutely Irreducible Models, Simple Spots.

By MASAYOSHI NAGATA.

In the present part of this sequence of papers, we want to study absolutely irreducible models and simple spots.

First, in Chapter 5, we study the extensions of ground rings and introduce the notion of absolutely irreducible models (§ 1). Then we introduce the notion of product models (§ 2) and fibre bundles (§ 3). And then we study the notion of absolutely normal spots (§ 4) and we introduce the notion of a point set attached to an absolutely irreducible models (§ 5). Furthermore, we define the notions of order of inseparability, cycles, divisors of functions, ideals of a model and line bundles (§§ 6-10).

Secondly, in Chapter 6, we first prove that the set of simple spots in a model forms a model (§ 1) and then we consider the Jacobian criterion of simplicity (§ 2) and we study the notion of absolutely simple spots (§ 3). In § 4 we prove that the set of absolutely normal spots in a model forms a model and then in § 5 we consider the notion of simple points. Finally, in § 6, we derive conditions for the simplicity of a tensor product of simple spots.

Results assumed to be known: Besides the results assumed to be known in previous parts of this sequence of papers and results in them, we assume that the results in [3] and [4] are known.

Chapter 5. Absolutely Irreducible Models.

1. Extension of ground rings. Let M be a model of a function field L over a ground ring I. Let I^* be a ground ring (not necessarily a ground ring of L) which contains I and let $\mathfrak{p}^*$ be a prime ideal of $L \otimes_I I^*$ such that $\mathfrak{p}^* \cap I = 0$. Let L^* be the field of quotients of $(L \otimes I^*)/\mathfrak{p}^*$. Then we can regard L and I^* as subrings of L^* in the natural way. (Then L^* is the field

* Received August 8, 1958.

of quotients of $I^*[L]$). Let $A_1, \cdots, A_n$ be affine models of L such that $M = \cup_i A_i$ and let $\mathfrak{o}_1, \cdots, \mathfrak{o}_n$ be affine rings of $A_1, \cdots, A_n$ respectively. Set $\mathfrak{o}^*_i = I^*[\mathfrak{o}_i]$. Then $\mathfrak{o}^*_i$ is an affine ring of L^* over I^*. Let A^*_i be the affine model defined by $\mathfrak{o}^*_i$ and set $M^* = \cup_i A^*_i$. Then

THEOREM 1. 1) *M^* is a model of L^* over I^*,* 2) *every spot in M^* dominates a spot in M and* 3) *M^* is the set of spots which are rings of quotients of $I^*[Q]$, where Q runs over all spots in M, hence M^* does not depend on the choice of the affine models A_i.*

This model M^* is called *an extension* of M over I^* *in the weak sense.* When $\mathfrak{p}^* = 0$, we call M^* *the extension* of M over I^* and M^* is denoted by $M \otimes I^*$.

Proof. Let Q^* be an arbitrary spot in M^* and let $\mathfrak{q}^*$ be the maximal ideal of Q^*. Q^* is a ring of quotients of some $\mathfrak{o}^*_i$, hence Q^* contains $\mathfrak{o}_i$. Therefore Q^* dominates $Q = (\mathfrak{o}_i)_{(\mathfrak{q}^* \cap \mathfrak{o}_i)}$, which proves 2) and we see that Q^* is a ring of quotients of $I^*[Q]$. Assume that $Q^{**} \in M^*$ corresponds to Q^*. Let Q' be a spot in M which is dominated by Q^{**}. Since there exists a place which dominates both Q^* and Q^{**}, hence also Q and Q', we see that Q corresponds to Q'. Since M is a model, $Q = Q'$. Therefore Q^* and Q^{**} are rings of quotients of the same ring $I^*[Q]$. By Lemma 2.1.1, we see that $Q^* = Q^{**}$, which proves 1), because M^* is the union of a finite number of affine models. We saw already that any spot Q^* in M^* is a ring of quotients of $I^*[Q]$ with $Q \in M$. Conversely, if $Q \in M$, then $I^*[Q]$ is a ring of quotients of some $\mathfrak{o}^*_i$ and therefore any spot Q^* which is a ring of quotients of $I^*[Q]$ is in M^*, and 3) is proved.

Remark 1. Let n be the transcendence degree of I^* over I (n may be infinite). If I is not a field and if I^* is a field, then

$$\dim M > \dim M^* \geqq \dim M - n - 1;$$

if both I and I^* are fields or if both I and I^* are not fields, then

$$\dim M \geqq \dim M^* \geqq \dim M - n.$$

Remark 2. If $\mathfrak{p}^*$ is a prime divisor of zero of $L \otimes I^*$, then $\dim M^*$ is equal to $\dim M$ or $\dim M - 1$, where the last case occurs when and only when I is not a field and I^* is a field. (For the proof, see Lemma 3.1.5.)

With the same L, L^* and I^*, let P be a spot of L (over I). Then a spot P^* which is a ring of quotients of $I^*[P]$ and which dominates P is called *an extension* of P over I^* *in the weak sense.* When $\mathfrak{p}^*$ is zero, P^* is called

an extension of P over I^*. By this definition, the extension of M over I^* is the set of extensions of spots in M over I^*.

In Chapter 2, we defined the notion of domination of models, which can be defined for models having different ground rings. If a model M^* dominates a model M, there exists a mapping f from M^* into M such that $f(P^*) = P$ $(P^* \in M^*, P \in M)$ if and only if P^* dominates P. This mapping f is called *the projection* or *the geometric projection* from M^* into M, which will be denoted by one of $\mathrm{proj}^{M^*}{}_M$, proj_M, proj.

Theorem 1 shows that from any extension of M even in weak sense the projection into M is well defined.

Assume that the extension $M \otimes I^*$ is defined. Then for a spot P in M, the set of spots P^* in $M \otimes I^*$ such that i) $\mathrm{proj}\, P^* = P$ and ii) $\mathrm{rank}\, P = \mathrm{rank}\, P^*$ is the set of rings of quotients of the local tensor product $P \times_I I^*$ with respect to its maximal ideals; such a P^* is called *a component* of $P \times I^*$. It will be easy to see that 1) if $Q^* \in M \otimes I^*$ and if $\mathrm{proj}\, Q^* = P$, then Q^* is a specialization of some component of $P \times I^*$ and 2) $P \times I^*$ is not defined if and only if there exists no ground place of I^* which dominates that ground place of I dominated by P.

We say that a model M over a ground ring I is *absolutely irreducible* if for any ground ring I^* containing I, the extension $M \otimes I^*$ is well defined, or equivalently, if the function field of M is a regular extension of I (by Theorem 3.3).

Remark. Let M be a normal model of a function field L over a ground ring I. Then every spot $P \in M$ contains the integral closure I' of I in L. Hence we may regard M as a model over I'. In this case, if L is separably generated over I, then L is a regular extension of I' (see Chapter 3, § 4) and M is an absolutely irreducible model over I'; if $I \neq I'$, then M is not an absolutely irreducible model over I.

LEMMA 1. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be rings containing a field k. If an element a of $\mathfrak{o}$ is not a zero divisor in $\mathfrak{o}$ then a is not a zero divisor in $\mathfrak{o} \otimes_k \mathfrak{o}'$.*

Proof. Let $\{v_i\}$ be a linearly independent k-base of $\mathfrak{o}'$. Assume that $ab = 0$ $(b \in \mathfrak{o} \otimes \mathfrak{o}')$ and $b = \sum a_i v_i$ $(a_i \in \mathfrak{o})$. Then $ab = 0$ means $\sum a a_i v_i = 0$, hence $a a_i = 0$ for all i. Therefore $a_i = 0$ and $b = 0$.

LEMMA 2. *Let $\mathfrak{o}$ and $\mathfrak{o}'$ be Noetherian rings containing a field k. Then any prime divisor of zero of $\mathfrak{o} \otimes_k \mathfrak{o}'$ is a minimal prime divisor of the ideal generated by some $\mathfrak{p}$ and $\mathfrak{p}'$ with $\mathfrak{p}$ and $\mathfrak{p}'$ prime divisors of zero in $\mathfrak{o}$ and $\mathfrak{o}'$ respectively.*

Proof. By the existence of a linearly independent k-base of $\mathfrak{o}'$, we see easily that if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathfrak{o}$, then

$$(\mathfrak{a} \cap \mathfrak{b})(\mathfrak{o} \otimes \mathfrak{o}') = \mathfrak{a}(\mathfrak{o} \otimes \mathfrak{o}') \cap \mathfrak{b}(\mathfrak{o} \otimes \mathfrak{o}').$$

Therefore we may assume that the zero ideal of $\mathfrak{o}$ is primary. Similarly, we assume also that the zero ideal of $\mathfrak{o}'$ is primary. Now, by Lemma 1, we may assume that the total quotient rings of $\mathfrak{o}$ and $\mathfrak{o}'$ coincide with $\mathfrak{o}$ and $\mathfrak{o}'$ respectively. Thus, we assume that $\mathfrak{o}$ and $\mathfrak{o}'$ are local rings of rank zero. If $\mathfrak{o}$ and $\mathfrak{o}'$ are fields, then the proof is easy (see the proof of Lemma 3.1.5). We shall use induction on length $\mathfrak{o}$ + length $\mathfrak{o}'$. Assume, for instance, that length $\mathfrak{o} > 1$. Let b be an element of $\mathfrak{o}$ such that $0 : b\mathfrak{o} = \mathfrak{p}$ with $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$. Let $\mathfrak{p}'$ be the maximal ideal of $\mathfrak{o}'$ and let $\mathfrak{p}^*_1, \cdots, \mathfrak{p}^*_n$ be all of the (minimal) prime divisors of the ideal generated by $\mathfrak{p}$ and $\mathfrak{p}'$. We have only to prove that if an element a of $\mathfrak{o} \otimes \mathfrak{o}'$ is not in any of the $\mathfrak{p}^*_i$, then a is not a zero divisor. Assume that $ac = 0$ with $c \in \mathfrak{o} \otimes \mathfrak{o}'$. By the induction assumption, a is not a zero divisor modulo $b(\mathfrak{o} \otimes \mathfrak{o}')$, hence $c \in b(\mathfrak{o} \otimes \mathfrak{o}')$. Let c' be an element of $\mathfrak{o} \otimes \mathfrak{o}'$ such that $c = bc'$. Then $ac' \in 0 : b(\mathfrak{o} \otimes \mathfrak{o}')$. By the existence of k-bases, we see easily that $0 : b(\mathfrak{o} \otimes \mathfrak{o}') = \mathfrak{p}(\mathfrak{o} \otimes \mathfrak{o}')$. Again by the induction assumption, a is not a zero divisor modulo $\mathfrak{p}(\mathfrak{o} \otimes \mathfrak{o}')$. Therefore we have $c' \in \mathfrak{p}(\mathfrak{o} \otimes \mathfrak{o}')$; hence $c = bc' = 0$. Therefore a is not a zero divisor, which proves our assertion.

LEMMA 3. *Let $\mathfrak{p}$ be a prime ideal of a spot P over a ground ring I and let I^* be a ground ring containing I. If $\mathfrak{p}^*$ is a prime divisor of the ideal $\mathfrak{p}(P \otimes_I I^*)$, then there exists a (minimal) prime divisor $\mathfrak{m}^*$ of the ideal of $P \otimes I^*$ generated by the maximal ideal $\mathfrak{m}$ of P such that $\mathfrak{p}^* \subseteq \mathfrak{m}^*$.*

Proof. Since $P \otimes I^*/\mathfrak{p}(P \otimes I^*) = (P/\mathfrak{p}) \otimes (I^*/(\mathfrak{p} \cap I)I^*)$, we may assume that $\mathfrak{p} = 0$. By Lemma 3.1.5, $\mathfrak{p}^*$ is a minimal prime divisor of zero. Assume that we know that $\mathfrak{p}^* + \mathfrak{m}(P \otimes I^*) \neq P \otimes I^*$. Since P is a ring of quotients of an affine ring over I, say $I[x_1, \cdots, x_n]$, $P \otimes I^*$ is a ring of quotients of $I^*[x_1, \cdots, x_n]$ $(= I[x_1, \cdots, x_n] \otimes I^*)$. $\mathfrak{p}^* \cap I^*[x_1, \cdots, x_n]$ is a minimal prime divisor of zero of $I^*[x_1, \cdots, x_n]$. Therefore the transcendence degree of $P \otimes I^*/\mathfrak{p}^*$ over I^* is that of P over I. Therefore, if $\mathfrak{q}^*$ is a prime ideal of $P \otimes I^*$ containing $\mathfrak{p}^*$ then rank $(\mathfrak{q}^*/\mathfrak{p}^*) =$ rank $\mathfrak{q}^*$. Now, let $y_1, \cdots, y_m$ be a system of parameters of P and let $\mathfrak{m}^*$ be a minimal prime divisor of $\mathfrak{p}^* + \sum y_i(P \otimes I^*)$. Then we have, by the above observation, rank $\mathfrak{m}^* \leqq m$. Since $\mathfrak{m}^*$ contains $\mathfrak{m}$, and since every prime ideal of $P \otimes I^*$ containing $\mathfrak{m}$ is of rank not less than m, we see that $\mathfrak{m}^*$ is a minimal prime divisor of $\mathfrak{m}(P \otimes I^*)$. Therefore it is sufficient to show that $\mathfrak{p}^* + \mathfrak{m}(P \otimes I^*)$

$\neq P \otimes I^*$, assuming that $\mathfrak{m}(P \otimes I^*) \neq P \otimes I^*$. For the purpose, we may assume that I^* is a ring of quotients of an affine ring over I. By Lemma 1, we may assume that I and I^* are ground places and I is dominated by P and I^*. If $x^*_1, \cdots, x^*_r$ are algebraically independent elements over I such that $I(x^*_1, \cdots, x^*_r)$ is dominated by I^*, then the zero ideal and the ideal $\mathfrak{m}(P \otimes I(x^*_1, \cdots, x^*_r))$ of $P \otimes I(x^*_1, \cdots, x^*_r)$ are obviously prime. Therefore, considering $(P \otimes I(x^*_1, \cdots, x^*_r))_{(\mathfrak{m})}$ and $I(x^*_1, \cdots, x^*_r)$ instead of P and I respectively, we may assume that I^* is a ring of quotients of an integral extension I' of I. (Therefore, if I is a field, then the proof is easy.) We first consider the case where $\operatorname{rank} P = 1$. Then $P \otimes I^*$ is a semi-local ring and every maximal ideal of $P \otimes I^*$ is of rank 1, as is easily seen. Therefore we see the proof of this case. Then the general case is proved by induction on rank P.

THEOREM 2. *Let M be a model of a function field L over a ground ring I and let I^* be a ground ring containing I.*

1) *If M is an absolutely irreducible model, then $M \otimes I^*$ (is well defined and) is an absolutely irreducible model over I^*.*

2) *Assume that $M \otimes I^*$ is well defined and let P be a spot in M. If an element f of $L \otimes I^*$ is in every component of $P \times I^*$, then f is in $P \otimes I^*$, provided that $P \times I^*$ is defined.*

Proof. 1) follows from Corollary 1 to Theorem 3.3. As for 2), we may assume that I is a ground place dominated by P. f is expressed in the form $\sum_1^n c_i w_i$ with $c_1, \cdots, c_n \in I^*$ which are linearly independent over I and with $w_i \in L$.

i) The case where I is a field: Let a be an element of P such that $aw_i \in P$ for any i $(a \neq 0)$. By Lemmas 2 and 3, we see that

$$\cap\ (aP_i \cap (P \otimes I^*)) = a(P \otimes I^*),$$

where P_i runs over all components of $P \times I^*$. Since $f \in P_i$, $af \in aP_i$. Therefore $af \in a(P \otimes I^*)$. Since a is not a zero divisor by Lemma 1, we have $f \in P \otimes I^*$.

ii) The case where I is not a field: Let p be a prime element of I. By case i) and by Lemma 3, the assertion is true for $P_\mathfrak{q}$ if $\mathfrak{q}$ is a prime ideal of P which does not contain p, i.e., $f \in \cap_\mathfrak{q} P_\mathfrak{q} \otimes I^*$ ($\mathfrak{q}$ runs over all prime ideals of P which do not contain p). Therefore there exists a power p^r of p such that $p^r f \in P \otimes I^*$. Choose r the smallest possible one. If $r = 0$, then

$f \in P \otimes I^*$. Assume the contrary. If $r > 1$, then considering $p^{r-1}f$, we may assume that $r = 1$. Then, since $P \otimes I^*/p(P \otimes I^*) = (P/pP) \otimes_{I/pI} (I^*/pI^*)$ and since I/pI is a field, we have $f \in P \otimes I^*$ as in the case i), which gives the proof for ii).

THEOREM 3. *If M is an absolutely irreducible model over a ground ring I, then for all but a finite number of prime ideals $\mathfrak{p}$ of I,* 1) *there exists only one general spot $P(\mathfrak{p})$ over $\mathfrak{p}$ in M,* 2) *$P(\mathfrak{p})$ is an unramified simple spot of rank* 1 *and* 3) *the induced model $\phi_{P(\mathfrak{p})}(M)$ is an absolutely irreducible model over $I/\mathfrak{p}$.*

Proof. When M is an affine model, the assertion is immediate from Theorem 3.6. As for the general case, let A be an affine model contained in M and let $\mathfrak{p}$ be a prime ideal of I. If one of the three conditions in our theorem is not true of $\mathfrak{p}$, then either there exists a general spot $P(\mathfrak{p})$ contained in $M - A$ or one of the conditions is not true with respect to A. Since $P(\mathfrak{p})$ is of rank 1, the first case is true only for a finite number of $\mathfrak{p}$, while by the case of affine models, the same is true for the second case. Therefore Theorem 3 is proved.

2. Product models. Let M and M' be models of function fields L and L' respectively over the same ground ring I. Assume that $L \otimes_I L'$ is an integral domain. (By Theorem 3.3, if one of M and M' is absolutely irreducible, then $L \otimes L'$ is an integral domain.) Let L^* be the field of quotients of $L \otimes L'$ and we regard L and L' as subfields of L^* in the natural way ($L^* = L(L')$). In this case, the join $J(M, M')$ of M and M' is called *the product model* of M and M' and will be denoted by $M \otimes M'$. When I is a field, $\dim (M \otimes M') = \dim M + \dim M'$; when I is not a field, $\dim M \otimes M' = \dim M + \dim M' - 1$.

PROPOSITION 1. 1) *If M and M' are affine models, then $M \otimes M'$ is also an affine model.* 2) *If M and M' are complete models, then $M \otimes M'$ is also a complete model.* 3) *If M and M' are projective models, then $M \otimes M'$ is also a projective model.*

The proof is immediate from the results in Chapter 2, § 4.

PROPOSITION 2. *When L and L' are imbedded in some other function field, then the join $J(M, M')$ in this case can be regarded as an induced model of $M \otimes M'$.*

Proof. Set $\mathfrak{S} = L[L']$ in the new imbedding. Then $\mathfrak{S}$ is a homomorphic

image of $L \otimes L'$. Let $\mathfrak{q}^*$ be the kernel of the homomorphism. On the other hand, let $\mathfrak{o}$ and $\mathfrak{o}'$ be affine rings whose affine models are contained in M and M' respectively. Set $\mathfrak{q} = \mathfrak{q}^* \cap (\mathfrak{o} \otimes \mathfrak{o}')$. Then $Q^* = (\mathfrak{o} \otimes \mathfrak{o}')_{\mathfrak{q}}$ is a spot in $M \otimes M'$. Since $L \otimes L'$ is a ring of quotients of $\mathfrak{o} \otimes \mathfrak{o}'$, we have $Q^* = (L \otimes L')_{\mathfrak{q}^*}$. Therefore we see easily that $J(M, M')$ is the induced model of $M \otimes M'$ defined by the spot Q^*.

PROPOSITION 3. *Let L, L' and L^* be the same as above ($L^* = L(L')$). Then a spot P of L corresponds to a spot P' of L' if and only if P and P' dominate the same ground place (of I).*

Proof. The only if part is obvious. Assume that P and P' dominate the same ground place I'. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be maximal ideals of P and P' respectively and let I'' be the residue class field of I'. Furthermore, let $\mathfrak{a}$ be the ideal of $P[P']$ $(= P \otimes P')$ generated by $\mathfrak{m}$ and $\mathfrak{m}'$. Then $P[P']/\mathfrak{a} = (P/\mathfrak{m}) \otimes_{I''} (P'/\mathfrak{m}')$, which shows that $\mathfrak{a}$ does not contain the identity. Therefore P corresponds to P' by Theorem 2.1.

COROLLARY. *Let M and M' be models over a ground ring I. Assume that $M \otimes M'$ is defined and that any ground place of I is dominated by some spots in M'. Then the projection from $M \otimes M'$ in M is an onto mapping.*

THEOREM 4. *Let M and M' be models over the same ground ring I. If one of M and M' is absolutely irreducible, then $M \otimes M'$ is well defined. If both M and M' are absolutely irreducible, then $M \otimes M'$ is also absolutely irreducible.*

The proof is immediate from the results in Chapter 3, § 4.

3. Definition of fibre bundles. Let M and F be models of function fields K and L respectively over the same ground ring I. Assume that $M \otimes F$ is well defined and let L^* be the function field of $M \otimes F$.

Let $\sigma_1, \cdots, \sigma_n$ be automorphisms of L^* over K and assume that there are models $A_1, \cdots, A_n$ of K such that

1) $M = \cup_i A_i$ and 2) $\sigma_i^{-1}\sigma_j((A_i \cap A_j) \otimes F) = (A_i \cap A_j) \otimes F$
for any (i, j). Then

THEOREM 5. *$M^* = \cup_i \sigma_i(A_i \otimes F)$ is a model of L^* over I.*

We call this model M^* *a fibre bundle* with *base model* M and *fibre* F; the σ_i's are called the *transition mappings* of M^* (defined on A_i's).

Proof. Since $A_i \otimes F$ is a model of L^*, $\sigma_i(A_i \otimes F)$ is also a model of L^*.

Therefore M^* is the union of a finite number of affine models. Assume that two spots P^* and P^{**} in M^* correspond to each other. Take i and j such that $P^* \in \sigma_i(A_i \otimes F)$, $P^{**} \in \sigma_j(A_j \otimes F)$. Let P' and P'' be the spots in M which are dominated by $\sigma_i^{-1}(P^*)$ and $\sigma_j^{-1}(P^{**})$ respectively. Since σ_i and σ_j are automorphisms over K, P^* and P^{**} dominate P' and P'' respectively, which shows that P' corresponds to P'' and therefore $P' = P''$. Therefore P' is in $A_i \cap A_j$. Therefore $\sigma_i^{-1}(P^*)$ and $\sigma_j^{-1}(P^{**})$ are in $(A_i \cap A_j) \otimes F$. Thus we have $P^* \in \sigma_i((A_i \cap A_j) \otimes F)$, $P^{**} \in \sigma_j((A_i \cap A_j) \otimes F)$. By our assumption, $\sigma_i((A_i \cap A_j) \otimes F) = \sigma_j((A_i \cap A_j) \otimes F)$. Therefore P^* and P^{**} are in the same model, hence $P^* = P^{**}$. Therefore M^* is a model.

When M^{**} is another fibre bundle with base model M and fibre F, we say that M^{**} is *equivalent* to M^* if there exists an automorphism σ of L^* over K such that $M^{**} = \sigma M^*$.

We shall show here that the notion of fibre variety in the sense of Weil [7] corresponds to our notion of the fibre bundle. A fibre variety W, with base V, fibre F, structure group G, transition functions s_{ij} and the field k of definition, is defined in the following manner:

V and F are abstract varieties and G is an automorphism group on F (for the definition, see Weil [7]), defined over k. $\{U_i\}$ is a finite covering of V by open sets in the sense of the k-topology. For each pair (i, j), s_{ij} is a rational mapping over k of V into G and defined at all points of $U_i \cap U_j$. For any triple (h, i, j), $s_{hj} = s_{hi} s_{ij}$ in $U_h \cap U_i \cap U_j$. Forming the union $\cup_i (U_i \times F)$, we define in this union the equivalence relation, denoted by $\sim$, namely; $(x, z) \sim (x', z')$ $((x, z) \in U_i \times F, (x', z') \in U_j \times F)$ if and only if $x = x'$ $(\in U_i \cap U_j)$ and $z' = s_{ji}(x) z$. Then the set W of equivalence classes becomes an abstract variety, which is birationally equivalent to $V \times F$.

We shall show that the set $S(W)$ of specialization rings of points of W over k is a fibre bundle in our sense, with base model $S(V)$ and fibre $S(F)$, where $S(V)$ and $S(F)$ are the sets of specialization rings of points in V and F respectively, over k. We denote by $S(U_i)$ the set of specialization rings of points of U_i over k. Let P and Q be independent generic points of V and F respectively, and let $(x) = (x_1, \cdots, x_m)$, $(z) = (z_1, \cdots, z_n)$ be the coordinates of representatives of P and Q in some affine representatives V' and F' of V and F respectively. Then we may regard $k(x)$, $k(z)$ and $k(x, z)$ as function fields of V, F and $V \times F$ respectively. Since $s_{ij}(x)$ is rational over $k(x)$ and is an automorphism of F, $s_{ij}(x) z$ is also in F and its coordinates (z') are rationally expressed in term of $k(x, z)$ and therefore the mapping $(z) \rightarrow (z')$ defines an automorphism of $k(x, z)$ over $k(x)$; that is, $s_{ij}(P)$ induces an automorphism of $k(x, z)$ over $k(x)$, which will be denoted by σ_{ij}.

On the other hand, the equivalence relation $\sim$ can be formulated as follows: We regard $s_{ij}(P)$ as a birational correspondence between $U_j \times F$ and $U_i \times F$ which maps $P \times Q$ to $P \times Q'$, where Q' is the point of F which has the representative $s_{ij}(x)z$ in F'. Then a point $R \times S$ in $U_i \times F$ is equivalent to $R' \times S'$ in $U_j \times F$ if and only if they are corresponding points under $s_{ij}(P)$. Therefore, the automorphism σ_{ij} of $k(x,z)$ identifies the specialization rings of equivalent points of $U_i \times F$ and $U_j \times F$. This shows also that $\sigma_{ij}((S(U_i) \cap S(U_j)) \otimes S(F)) = (S(U_i) \cap S(U_j)) \otimes S(F)$. Since $s_{hj} = s_{hi}s_{ij}$, we have, fixing one h, say 1, $\sigma_{ij} = \sigma_{1i}^{-1}\sigma_{1j}$. Therefore, if we denote σ_{1j} by σ_j, then we see that $S(W)$ is a fibre bundle in our sense with base $S(V)$, fibre $S(F)$ and the transition mappings σ_i.

4. Absolutely normal spots. A spot P over a ground ring I is called *absolutely normal* if 1) P is a regular extension of I and 2) for any ground ring I^* containing I (and such that $P \times I^*$ is defined), every extension of P over I^* is normal. Observe that I^* may be restricted only to fields or valuation rings which dominate the ground place of I dominated by P and whose field of quotients is finitely generated over that of I.

A model M is called *absolutely normal* if every spot of M is absolutely normal.

A spot P over a ground ring I is called *weakly absolutely normal* if 1) P is a regular extension of I and 2) if I^* is a ground ring which is also a valuation ring (or a field) unramified over the ground place I' of I dominated by P (i.e., the maximal ideal of I' generates that of I^*), then every extension of P over I^* is normal.

If we consider only models over fields, then weak absolute normality coincides with absolute normality. Furthermore,

PROPOSITION 3. *Let P be a weakly absolutely normal spot over a ground ring I. If P contains the field of quotients of I, then P is absolutely normal.*

Proof. We may assume that I is a field. If P is not absolutely normal, then there exists a ground ring I^* containing I such that 1) some extension of P over I^* is not normal and 2) the field of quotients K of I^* is finitely generated over I. Let k be a finite purely inseparable extension of I such that $k(K)$ is separably generated over k. By the assumption, $P[k] = P \otimes k$ is a normal spot over k. Let I^{**} be the integral closure of I^* in $k(K)$. Since both $P[k]$ and I^{**} are separably generated over the field k and since they are normal rings, $P[k] \otimes_k I^{**}$ is a normal ring by Theorem 3.8. This

contradicts the assumption that there is an extension of P over I^* which is not normal; for, $P[k]\otimes_k I^{**}=P\otimes_I I^{**}=(P\otimes_I I^*)\otimes_{I^*} I^{**}$.

THEOREM 6. *Let P be a normal spot over a ground place dominated by P. If P is a regular extension of I and if I and the residue class field k of I are perfect, then P is weakly absolutely normal.* (*In this case, I is either a field or a ring of characteristic zero.*)

Proof. If I is a field, then the assertion follows by Theorem 3.8. Assume that I is not a field. Let I^* be a ground place dominating I and unramified over I. Let x be a prime element of I. Set $\mathfrak{o}^*=P\otimes I^*$ and let $\mathfrak{p}^*$ be a prime divisor of $x\mathfrak{o}^*$. Since $\mathfrak{o}^*/x\mathfrak{o}^*=(P/xP)\otimes_{I/xI} I^*/xI^*$, $x\mathfrak{o}^*$ has no imbedded prime divisors, hence $\mathfrak{p}^*$ is a minimal prime divisor of $x\mathfrak{o}^*$. Set $\mathfrak{p}=\mathfrak{p}^*\cap P$. Then $\mathfrak{p}$ is a minimal prime divisor of xP. Since I^*/xI^* is a separably generated extension of I/xI, $P/\mathfrak{p}\otimes I^*/xI^*$ has no nilpotent elements. Therefore, if y is a prime element of $P_{\mathfrak{p}}$, then $\mathfrak{p}^*\mathfrak{o}^*_{\mathfrak{p}^*}$ is generated by y, which proves that $\mathfrak{o}^*_{\mathfrak{p}^*}$ is a normal ring. Therefore by Proposition 3.9, the assertion follows.

COROLLARY 1. *Let P be a spot over a field k such that P is a regular extension of k. If there exists a field K containing k such that at least one extension of P over K is absolutely normal, then P is absolutely normal.*

Proof. Let k^* be the smallest perfect field containing k. We may assume that K contains k^*. Since there exists only one extension P^* of P over k^*, P^* must be normal, hence P^* is absolutely normal by Theorem 6, which shows that P is absolutely normal.

COROLLARY 2. *Let P be a spot over a field k such that P is a regular extension of k. Then P is absolutely normal if and only if $P[k']$ is normal for any finite purely inseparable extensions k' of k, or equivalently, for the smallest perfect field k' containing k.*

LEMMA 1. *Let P be a normal spot over a ground ring I and let x be a prime element of the ground place I' dominated by P. Assume that $x\neq 0$. Then P is absolutely normal if and only if $P_{\mathfrak{p}}$ is absolutely normal for any prime ideal $\mathfrak{p}$ which does not contain x and also for any (minimal) prime divisor $\mathfrak{p}$ of xP.*

Proof. The only if part is obvious (more generally, if a spot is not absolutely normal, then its specialization is not absolutely normal, as is easily seen). We assume that $P_{\mathfrak{p}}$ is absolutely normal for any prime $\mathfrak{p}$ as stated

above. Let I^* be a ground ring, which is a valuation ring and which dominates I'. By the assumption, for $\mathfrak{p}$ which do not contain x, we see that $(P\otimes I^*)[1/x]$ is a normal ring. On the other hand, since

$$P\otimes I^*/x(P\otimes I^*)=(P/xP)\otimes_{I/xI}I^*/xI^*,$$

$x(P\otimes I^*)$ has no imbedded prime divisor by Lemma 5.1.2. Therefore, the absolute normality of $P_\mathfrak{p}$ for minimal prime divisors of xP shows that for any prime divisor $\mathfrak{p}^*$ of $x(P\otimes I^*)$, $(P\otimes I^*)_{\mathfrak{p}^*}$ is a normal ring. Therefore we see that $P\otimes I^*$ is a normal ring.

LEMMA 2. *Let $\mathfrak{v}$, $\mathfrak{v}'$ and I be discrete (rank 1) valuation rings having prime elements x, x' and y respectively. Assume that I is dominated by $\mathfrak{v}$ and $\mathfrak{v}'$ and that $y\mathfrak{v}\neq x\mathfrak{v}$, $y\mathfrak{v}'\neq x'\mathfrak{v}'$. Then $\mathfrak{v}\otimes_I\mathfrak{v}'$ cannot be a normal ring.*

Proof. Let e and e' be such that $y\mathfrak{v}=x^e\mathfrak{v}$, $y\mathfrak{v}'=x'^{e'}\mathfrak{v}'$. We may assume that $e\leqq e'$. If $\mathfrak{v}\otimes\mathfrak{v}'$ is a normal ring, it is the intersection of valuation rings containing it. For any valuation v whose valuation ring contains $\mathfrak{v}\otimes\mathfrak{v}'$, $ev(x)=v(y)=e'v(x')$. Therefore $v(x)\geqq v(x')$, hence $x/x'\in\mathfrak{v}\otimes\mathfrak{v}'$, which is obviously impossible.

As a corollary to this lemma, we have

PROPOSITION 4. *If a spot P over a ground ring I is absolutely normal and if $\mathfrak{p}$ is a prime ideal of rank 1 in P such that $\mathfrak{p}\cap I\neq 0$, then $\mathfrak{p}P_\mathfrak{p}=(\mathfrak{p}\cap I)P_\mathfrak{p}$;* i.e., *$P_\mathfrak{p}$ is an unramified simple spot.*

THEOREM 7. *A spot P over a ground ring I is absolutely normal if (and only if) $P\otimes_I I^*$ is normal for any finite normal extension I^* of I; if I is of positive characteristic, then we may restrict I^* to purely inseparable extensions.*

Proof. By virtue of Corollary 1 to Theorem 6, we may assume that I is a valuation ring ($\neq$ a field) which is dominated by P. Let y be a prime element of I. Lemma 2 shows that y is a prime element of $P_\mathfrak{p}$ if $\mathfrak{p}$ is a prime ideal of rank 1 such that $\mathfrak{p}\cap I\neq 0$. Let K be any discrete valuation ring dominating I whose field of quotients is finitely generated over that of I. Let I' be a finite purely inseparable normal extension of I such that $K[I']$ is separably generated over I'. In order to prove the normality of $P\otimes K$, considering $P\otimes I'$ instead of P, we may assume that K is separably generated over I. Let p be the characteristic of I/yI. Let I^* be as follows: 1) If I/yI is perfect, then $I^*=I$. 2) When I/yI is not perfect, let $\{a_\sigma\}$ be a p-base of I/yI (i.e., a maximal set of p-independent elements of I/yI) and let b_σ be

a representative of a_σ for every σ. Then I^* is the ring generated by all p-power roots of b_σ over I (for all σ). Then I^* is a valuation ring and yI^* is the maximal ideal. Furthermore, I^*/yI^* is the smallest perfect field containing I/yI. Since I^* is algebraic over I, we see that $P \otimes I^*$ is a normal ring and by the same reason $y(P \otimes I^*)$ is semi-prime. Let K^* be an extension of K in the field generated by K and I^*. Then K^* is discrete, because of finite generation of K and by our construction of I^*. Let $\mathfrak{p}^*$ be any prime divisor of $y(P \otimes K^*)$. By Lemma 5.1.2, we see that $\mathfrak{p}^*$ is minimal. Since y is in x^*K^*, we see that

$$P \otimes K^*/x^*(P \otimes K^*) = (P \otimes I^*/y(P \otimes I^*)) \otimes_{I^*/yI^*} K^*/x^*K^*.$$

This shows that $x^*(P \otimes K^*)$ is semi-prime, because I^*/yI^* is a perfect field and because $y(P \otimes I^*)$ is semi-prime. Therefore $\mathfrak{p}^*(P \otimes K^*)_{\mathfrak{p}^*}$ is generated by x^*, hence $(P \otimes K^*)_{\mathfrak{p}^*}$ is a valuation ring. Therefore we have $P \otimes K^*$ is a normal ring by Proposition 3.9, and therefore $P \otimes K$ is a normal ring. Thus the assertion is proved.

THEOREM 8. *If P and P' are absolutely normal spots over the same ground ring I and if I^* is a ground ring containing I, then $P \otimes_I P' \otimes_I I^*$ is a normal ring.*

Proof. Since every spot which as P or P' as a specialization is also absolutely normal, we may assume that I and I^* are valuation rings (or fields). 1) When I is a field, let k be the smallest perfect field containing I, then $P \otimes k$, $P' \otimes k$ are absolutely normal, and we may assume that I is perfect. Then Theorem 3.8 shows the normality of $P \otimes P' \otimes I^*$. 2) When I is not a field, let p be a prime element of I. Then by the case I a field, $(P \otimes P' \otimes I^*)[1/p]$ is a normal ring. For any prime divisor $\mathfrak{p}'$ of $p(P' \otimes I^*)$, $(P' \otimes I^*)_{\mathfrak{p}'}$ is a ground ring. Therefore for any prime divisor $\mathfrak{p}^*$ of $p(P \otimes P' \otimes I^*)$, $(P \otimes P' \otimes I^*)_{\mathfrak{p}^*}$ is a normal ring. It follows now that $P \otimes P' \otimes I^*$ is a normal ring.

COROLLARY. *If M and M' are absolutely normal models over the same ground ring, then $M \otimes M'$ is also absolutely normal.*

By the same proof as for Theorem 8, we have

PROPOSITION 5. *Let P and P' be normal spots over a ground ring I. If one of P and P' is absolutely normal and if the other is separably generated over I, then $P \otimes P'$ is a normal ring.*

5. Point set attached to an absolutely irreducible model—the notion of varieties. Let I be a ground ring and let U be a set of infinitely many algebraically independent elements over I. Then the integral closure of $I(U)$ in the algebraic closure of the field of quotients of $I(U)$ in the algebraic closure of the field of quotients of $I(U)$ is called the *universal domain* of I with respect to the set U.

We shall fix the set U and the universal domain D with respect to U, unless the contrary is explicitly stated.

A ground ring I^* which contains I is called a *canonical extension* of I if I^* is a finite integral extension of $I(U')$ with a subset U' of U. Observe that if $U-U'$ is a infinite set, then D is the universal domain of I^* with respect to $U-U'$

Now let M be an absolutely irreducible model over I. Let $\{I_\sigma; \sigma \in \Sigma\}$ be the set of all canonical extensions of I (in D). Then the extensions $M_\sigma = M \otimes I_\sigma$ are defined and the set of M_σ forms an inverse system under projection. Let M' be the limit of this inverse system. A member of M' is called a *point* of M and M' is called the *variety* of M (with respect to U).

If P is a point of M, then there exists a uniquely determined spot P_σ in M_σ which is a representative of P in M_σ (for each $\sigma \in \Sigma$). This P_σ is called the spot of P over I_σ. When $\dim P_\sigma = n$, we say that P is a point of *dimension* n over I_σ. If $\dim P_\sigma = \dim M_\sigma$, we say that P is a *generic point* of the variety M' over I_σ.

Remark. The above notion of points does not coincide with the usual notion of points of a variety; the points in our sense contains also generic points of subvarieties over the universal domain, namely, if I is a field then M' is nothing but the extension of M over the universal domain.

Let P and Q be points of the variety M' and let P_σ and Q_σ be spots of P and Q over I_σ. Then we say that Q is a *specialization* of P over I_σ if Q_σ is a specialization of P_σ.

Let P be a spot in M. If the induced model $\phi_P(M)$ is absolutely irreducible over $\phi_P(I)$ and if $\phi_P(I) = I$, then the set of points of the variety M', whose spots over I are in $M(P)$ can be naturally identified with the variety of $\phi_P(M)$, which is called the *subvariety* of M' attached to the spot P and we say that the subvariety is defined over I. Similarly for M_σ, we defined the notion of subvarieties defined over I_σ.

Let $\mathfrak{p}$ be a prime ideal of I. If $\mathfrak{p}'$ is a prime ideal of the universal domain D such that $\mathfrak{p}' \cap I = \mathfrak{p}$, then we say that $D_{\mathfrak{p}'}$ is a universal place over $\mathfrak{p}$ (or $I_{\mathfrak{p}}$). Now, if, for a $P \in M$, $\phi_P(M)$ is absolutely irreducible over

$\phi_P(I)$ and if $\phi_P(I) \neq I$, then the following subset M'' is naturally identified with the variety of $\phi_P(M)$:

Let $I_{\mathfrak{p}}$ be the ground place dominated by P and let D' be a universal place over $I_{\mathfrak{p}}$. Let M'' be the set of points Q of M' such that i) the spot of Q over I is in $M(P)$ and ii) the spot of Q over I_σ dominates the ground place of I_σ dominated by D' (for all $\sigma \in \Sigma$).

We call M'' a *representative* of the subvariety of M' attached to P and we say that M'' is defined over $\phi_P(I)$. The union of all M'' (for all possible choice of D') is called the *subvariety* of M attached to P and we say that the subvariety is *defined* over I.

The same can be observed for M_σ.

If F is a closed set of M_σ, then the set of points whose spots over I_σ are in F is called the *closed set* of M' attached to F. For a fixed I_σ, all possible such sets are defined to be the closed sets of M' in *I_σ-topology* of M'; it will be easy to see that this really defines a topology in M'. The closed set attached to an irreducible closed set of M_σ is called a *relatively irreducible* subvariety of M' defined over I_σ.

Let L be the function field of M. Then an element f of the field of quotients of $L \otimes D$ is called a *function* on the variety M'; if f is in the field of quotients of $L \otimes I_\sigma$, then we say that f is *defined* over I_σ. A function f which is defined over I_σ is said to be regular at a point P if f is in the spot of P over I_σ (observe that this is independent of I_σ whenever f is defined). P defined a uniquely determined homomorphism $\lim \phi_{P_\sigma}$, which is denoted by ϕ_P. Then $\phi_P(f)$ is defined if and only if f is regular at P; in this case $\phi_P(f)$ is called the *value* of f at P.

When M is an affine model defined by the affine ring $I[x_1, \cdots, x_n]$, the system $(x_1, \cdots, x_n)$ is called a *coordinate system* of the variety M'. If P is a point of M', then the x_i is regular at P. The system $(\phi_P(x_1), \cdots, \phi_P(x_n))$ is called the coordinates of P attached to the coordinate system $(x_1, \cdots, x_n)$.

When M is a projective model defined by homogeneous coordinates $(z_0, \cdots, z_n)$, we say that $(z_0, \cdots, z_n)$ is a *homogeneous coordinate system* of M' and we say that M' is a *projective variety*. If P is a point of M', then there exists one i such that z_j/z_i is regular at P for every j. Then, t being an arbitrary non-zero element of the set of values of regular functions at P, the system $(t\phi_P(z_0/z_i), \cdots, t\phi_P(z_n/z_i))$ is called *homogeneous coordinates* of P.

Let P be a point of the variety M' and let P_σ be the spots of P over I_σ. (1) P is called a *simple point* of M' if every P_σ is a simple spot; otherwise,

P is called a *singular* point. (2) P is called a *normal point* if every P_σ is a normal spot.

THEOREM 9. *With the same notations as above, the following three conditions are equivalent to each other:*

(1) *P is a normal point.*

(2) *Every P_σ is absolutely normal.*

(3) *There exists one I_σ such that P_σ is absolutely normal.*

Proof. Let I be I_0. i) Assuming (1), we shall prove (2). It will be sufficient to show that P_0 is absolutely normal. If P_0 is not absolutely normal, then there exists a finite normal extension I_σ of I such that one extension of P_0 over I_σ is not normal. Since I_σ is a normal extension of I, extensions of P_0 over I_σ are conjugate to each other, hence P_σ is not normal, which is a contradiction. Thus P_0 is absolutely normal, and every P_σ is absolutely normal. ii) It is obvious that (3) follows from (2). iii) Assuming (3), we shall prove (1). It is obvious that if $I_{\sigma'}$ contains I_σ, then $P_{\sigma'}$ is also absolutely normal. Since for any given $I_{\sigma''}$, there exists an $I_{\sigma'}$ which contains both I_σ and $I_{\sigma''}$, we see that $P_{\sigma''}$ is a normal spot, which shows that P is a normal point. Thus the theorem is proved.

Similar assertion for simple points will be proved in the next chapter.

6. The order of inseparability. Throughout this section, let L be a function field over a ground field k, let $(x) = (x_1, \cdots, x_n)$ be an arbitrary transcendence base of L over k, let $\mathfrak{o}$ be a local ring of rank zero which contains k, let $\mathfrak{n}$ be the maximal ideal of $\mathfrak{o}$, let k' be the residue class field $\mathfrak{o}/\mathfrak{n}$ and let $(u) = (u_1, \cdots)$ be a transcendence base of k' over k.

Obviously, $L \times_k \mathfrak{o}$ is the direct sum of a finite number of local rings of rank zero. When a local ring $\mathfrak{S}$ is a direct summand of $L \times_k \mathfrak{o}$, then the length $l(\mathfrak{S})$ of $\mathfrak{S}$ is denoted by $i(L/k; \phi_{\mathfrak{S}}(\mathfrak{S})/\mathfrak{o})$. If $i(L/k; \phi_{\mathfrak{S}}(\mathfrak{S})/\mathfrak{o})$ does not depend on the choice of direct summand, it is called the *order of inseparability* of L *over* $\mathfrak{o}$ and is denoted by $i(L/k; \mathfrak{o})$. Observe that if $\mathfrak{o}$ is the algebraic closure of k, then $i(L/k; \mathfrak{o})$ is the *order of inseparability* $[L: k]_i$ of L (in the sense of Weil [6]), as is easily seen by the following

THEOREM 10. *$\mathfrak{S}' = \mathfrak{S}/\mathfrak{n}\mathfrak{S}$ is a direct summand of $L \times_k k'$, and*

$$i(L/k; \phi_{\mathfrak{S}}(\mathfrak{S})/\mathfrak{o}) = l(\mathfrak{o}) \cdot i(L/k; \phi_{\mathfrak{S}}(\mathfrak{S})/k').$$

Furthermore,

$$i(L/k; \phi_{\mathfrak{S}}(\mathfrak{S})/k') = [L: k(x)]_i/[\phi_{\mathfrak{S}}(\mathfrak{S}): k'(x)]_i.$$

On the other hand, if P is a spot over a ground place I, $\mathfrak{m}$ and $\mathfrak{n}'$ are maximal ideals of P and I respectively, I^* is a ground ring containing I, P' is a component of $P \times_I I^*$, $P/\mathfrak{m} = L$, $I/\mathfrak{n}' = k$, $\mathfrak{o} = I^*/\mathfrak{n}'I^*$ and $\mathfrak{S} = P'/\mathfrak{n}'P'$, then

$$i(L/k; \phi_{\mathfrak{S}}(\mathfrak{S})/\mathfrak{o}) = e(\mathfrak{m}P')/e(\mathfrak{m}).$$

Proof. The first formula can be proved easily by induction on the length of $\mathfrak{o}$. We shall prove now the second formula. Since $L \times_k k' = L(u) \times_{k(x,u)} K(x)$ and since $[L : k(x)]_i = [L(u) : k(x,u)]_i$, we may assume that L and k' are algebraic over k. Let k'' be the maximal separable extension of k contained in k' and let L'' be the direct summand of $L \times k''$ contained in $\mathfrak{S}'$. Then L'' is a field and is separable over L. Therefore, considering L'' and k'' instead of L and k, we may assume that k' is purely inseparable over k. By the same reason, we may assume furthermore that L is purely inseparable over k, and we have a proof of this case easily. Lastly we shall prove the third formula. By the same reason as above (observing residue class fields), we may assume that the residue class fields of P, I^* are algebraic over that of I. On the other hand, we may assume that I^* is also a ground place dominated by P'. Then extending P and P' over the completions of I and I^* respectively, we may assume that I and I^* are complete (observe that the invariance of the multiplicities under the extensions follows from Proposition 2 in Appendix 2 in Part II of the present sequence of papers). Again by the same reason as for the second formula, we may assume that the residue class fields of P and I^* are purely inseparable over that of I. Now, if the residue class field k' of I^* is finite over $k = I/\mathfrak{n}'$, namely, if I^* is finite over I (because I is complete), then by the extension formula for multiplicity, we see that $e(\mathfrak{m}P')/e(\mathfrak{m}) = [L : k]/[\phi_{P'}(P') : k']$, hence by the second formula we have the required formula. Now the general case (where I^* is not finite over I) can be reduced easily from the case where I^* is finite over I.

COROLLARY. *Under the same notations as above,* (i) *if $\mathfrak{o}$ is a field and if one of L and $\mathfrak{o}$ is separably generated over k then $i(L/k; \mathfrak{o}) = 1$ and* (ii) *L is separably generated over k if and only if $[L : k]_\iota = 1$.*

By virtue of the first part of Theorem 10, we see that the case where $\mathfrak{o}$ is a field is fundamental and we shall consider this case.

THEOREM 11. *Let L' be a function field over k containing L and let k'' be a field containing k'. Assume that they are contained in a field and that $\dim_k L' = \dim_{k''} k''(L')$. Then we have*

(i) $i(L/k\,;k''(L)/k'')=i(L/k\,;k'(L)/k')\cdot i(k'(L)/k'\,;k''(L)/k'')$,

(ii) $i(L'/k\,;k'(L')/k')=i(L/k\,;k'(L)/k')\cdot i(L'/L\,;k'(L')/k'(L))$.

Proof. We shall prove (i) first. Let (u'') be a transcendence base of k'' over k'. Then by the same reason as in the proof of Theorem 10, we may consider $k(u,u'')$ and $k'(u'')$ instead of k and k' respectively and we may assume that k'' is an algebraic extension of k. Similarly, we may assume that L is algebraic over k. Then just as in the proof of Theorem 10, we may assume that L, k' and k'' are purely inseparable over k. Then, in this case, $i(L/k\,;k''(L)/k'')=l(L\otimes_k k'')$, $i(L/k\,;k'(L)/k')=l(L\otimes_k k')$ and $i(k'(L)/k'\,;k''(L)/k'')=l(k'(L)\otimes_{k'} k'')$. Therefore the formula follows from the fact that $L\otimes_k k'=(L\otimes_k k')\otimes_{k'} k''$. Now we consider (ii). Just as above, we may assume that k' and L' are purely inseparable over k. Then we prove the formula by the fact that $L'\otimes_k k'=L'\otimes_L(L\otimes_k k')$.

COROLLARY. *If furthermore L'' is a field containing $k'(L)$ and if $\dim_L L'=\dim_{L''} L'(L'')$ and $k'(L')\subseteq L'(L'')$, then*

$$i(L'/k\,;k'(L')/k')/i(L/k\,;k'(L)/k')$$
$$=i(L'/L\,;L'(L'')/L'')/i(k'(L')/k'(L)\,;L'(L'')/L'').$$

In particular,

$$[L'\colon k]_\iota/[L\colon k]_\iota=[L'\colon L]_\iota/[\bar{k}(L')\colon \bar{k}(L)]_\iota,$$

where $\bar{k}$ is the algebraic closure of k.

Proof. Both sides of the first formula are equal to $i(L'/L\,;k'(L')/k'(L))$. The second formula follows from the first one as the special where $k'=\bar{k}$ and L'' is the algebraic closure of L.

As applications of our treatment, we shall show how Propositions 29-31 in Weil [6, Chapter I] can be proved.

PROPOSITION 6. *Let L be a function field over a field k of characteristic $p\neq 0$. If m is the natural number such that $[L\colon k]_\iota=p^m$ $(\neq 1)$, then $i(L/k\,;k^{1/p})>1$ (hence $\geqq p$) and $L(k^{p^{-m}})$ is separably generated over $k^{p^{-m}}$, i.e., $i(L/k\,;k^{p^{-m}})=p^m$* (Weil [6]).

Proof. Since L is not separably generated over k, $L\otimes k^{1/p}$ is not an integral domain and therefore $i(L/k\,;k^{1/p})>1$. Hence

$$[L(k^{1/p})\colon k^{1/p}]_\iota=[L\colon k]_\iota/i(L/k\,;k^{1/p})=p^n \text{ with } n<m.$$

Therefore we have $[L(k^{p^{-m}})\colon k^{p^{-m}}]_\iota=1$, $i(L/k\,;k^{p^{-m}})=p^m$.

PROPOSITION 7. *Assume that* $L = k(x_1, \cdots, x_r, x_{r+1})$ *and that* $\dim_k L = r$. *Assume furthermore that* $[L : k]_\iota = p^m$. *Let* $\bar{k}$ *be the algebraic closure of* k *and let* F, G, H *be the irreducible polynomials in indeterminates* $X_1, \cdots, X_{r+1}$ *for* $(x_1, \cdots, x_{r+1})$ *over* k, $k^{p^{-m}}$, $\bar{k}$ *respectively. Then we have, except for constant factors,* $F = G^{p^m}$ *and* $G = HH'$ *with a polynomial* H' *over* $\bar{k}$ *such that* $H'(x_1, \cdots, x_{r+1}) \neq 0$ (Weil [6]).

Proof. Set $A = k[X_1, \cdots, X_{r+1}]$. Then A/FA is an affine ring of L. By Proposition 6, $l(L \otimes k^{p^{-m}}) = p^m$. This shows that, denoting by A' the ring $A[k^{p^{-m}}]$, we have $FA' = G^{p^m}A'$ because $k^{p^{-m}}$ is purely inseparable over k. As for the last assertion, we have, denoting by $\bar{A}$ the ring $A[\bar{k}]$, $G\bar{A}$ is semi-prime because $[L(k^{p^{-m}}) : k^{p^{-m}}]_\iota = 1$.

In order to apply our observation in this section to absolutely irreducible models, we shall introduce another notation as follows:

Let P be a spot over a ground ring I and assume that P is a regular extension of I. Let I' be a ground ring containing I. Assume that P' is a component of $P \times_I I'$. Let $\mathfrak{m}$ be the maximal ideal of P. Then $i(P/I; P'/I')$ denotes the length $l(P'/\mathfrak{m}P')$, which is equal to $e(\mathfrak{m}P')/e(\mathfrak{m})$ (by Theorem 10) and also to $i((P/\mathfrak{m})/(I/(\mathfrak{m} \cap I))\,;\,(\phi_{P'}(P'))/(I'_{\mathfrak{p}'}/(\mathfrak{m} \cap I)I'_{\mathfrak{p}'})$ where $I'_{\mathfrak{p}'}$ is the ground place of I' dominated by P'.

7. The definition of cycles. Let M be an absolutely irreducible model over a ground ring I. An element Z of the free module generated by all spots of M over the field of rational numbers is called a *generalized cycle* on M. For a generalized cycle $Z = \sum c_i P_i$ $(P_i \in M)$, (i) each P_i whose coefficient c_i is different from zero is called a *component* of Z and (ii) the union of the loci of the components of Z is called the *carrier* of Z and is denoted by $\operatorname{Supp} Z$.

A generalized cycle Z is said to be *effective*, and is denoted by $Z \succ 0$, if the coefficient of every component of Z is positive (Z may be zero). For two generalized cycles Z and Z', if $Z - Z'$ is effective, then we write $Z \succ Z'$. Then the relation $\succ$ gives a partial order in the group of generalized cycles on a model.

For a generalized cycle Z, there are effective generalized cycles Z_+ and Z_- such that 1) $Z = Z_+ - Z_-$ and 2) Z_+ and Z_- have no common components. Such Z_+ and Z_- are uniquely determined. Z_+ and Z_- are called the *positive part* and the *negative part* of Z respectively.

An *integral cycle* is a generalized cycle whose coefficients are all integers. A *cycle* is an integral cycle whose components are absolutely simple. A cycle

(or a generalized cycle or an integral cycle) is called an *r-cycle* (or a generalized r-cycle or an integral r-cycle) if its components are all of dimension r; it is said to be *unmixed* if furthermore all components dominate the same ground place.

A $(\dim M - 1)$-cycle on M is called a *divisor*; a *generalized divisor* and an *integral divisor* are defined similarly.

A spot in M can be regarded as a generalized cycle (an integral cycle) on M; it is said to be *prime*; thus we define generalized prime cycles, prime cycles, prime divisors and so on.

Let I^* be a ground ring containing I. For a generalized cycle $Z = \sum c_j P_j$ on M, let $\sigma(Z)$ be $\sum c_j \cdot i(P_j/I; P^*_{jl}/I^*) P^*_{jl}$, where P^*_{jl} runs over all components of $P_j \times I^*$ for each j. This σ defines a homomorphism from the group of generalized cycles on M into that of $M \otimes I^*$, which will be denoted by $\sigma_{I^*/I}$. Observe that if I^* is a canonical extension of I then $\sigma_{I^*/I}$ is an isomorphism. By our definition, it follows easily from Theorems 10 and 11 that

THEOREM 12. *If I, I^* and I^{**} are ground rings such that $I \subseteq I^* \subseteq I^{**}$, then* $\sigma_{I^{**}/I} = \sigma_{I^{**}/I^*} \cdot \sigma_{I^*/I}$.

Observe that $\sigma_{I^*/I}$ preserves the properties of being an integral cycle, of being a cycle, and so on. Therefore, when we consider canonical extensions of I, cycles, generalized cycles, integral cycles, and so on, on M can be identified with those on the extensions of M, and therefore we can define generalized cycles, cycles, r-cycles, integral cycles on the variety of M with respect to a universal domain, hence we can define also I-rational cycles, I-rational integral cycles, and so on, on the variety.

If M' is a model contained in M, then the following mapping ϕ is a homomorphism from the group of generalized cycles on M onto that of M': $\phi(\sum c_i P_i) = \sum_{P_i \in M'} c_i P_i$. This mapping ϕ is called the *restriction* on M' and is denoted by $[\ ]_{M'}$, namely,

$$[\sum c_i P_i]_{M'} = \sum_{P_i \in M'} c_i P_i.$$

8. Divisor of a function. We shall define at first the notion of algebraic projection in a special case (the general definition will be given in Part IV of the present sequence of papers).

Let M be a model of a function field L over a ground ring I and let L' be a finite algebraic extension of L. Assume that a model M' of L' dominates M and is dominated by the derived normal model $N(M; L')$ of M in L' and that L' is a regular extension of I (hence L is also a regular extension of I).

The *algebraic projection* $\mathrm{pr}^{M'}{}_M$ (or pr) from M' into M is defined by the following conditions: (1) If $P' \in M'$, then, denoting by P the projection of P' on M, $\mathrm{pr}\,P' = [\phi_{P'}(P') : \phi_P(P)]P$ (this is an integral cycle on M) and (2) pr is a homomorphism from the group of generalized cycles on M' into that on M. From this definition, it follows immediately that

PROPOSITION 8. *If* $\mathrm{pr}^{M''}{}_{M'}$ *and* $\mathrm{pr}^{M'}{}_M$ *are defined, then* $\mathrm{pr}^{M''}{}_M$ *is also defined and coincides with* $\mathrm{pr}^{M''}{}_{M'} \cdot \mathrm{pr}^{M'}{}_M$.

Now let M, L and I be as above. Let $f \neq 0$ be a function on M (i.e., $f \in L$) and let $N(M)$ be the derived normal model of M. For any spot P' of rank 1 in $N(M)$, let $v_{P'}$ be the normalized valuation defined by P'. Then $(f)_{N(M)} = \sum v_{P'}(f)P'$ (P' runs over all spots P' of rank 1 in $N(M)$) is an integral divisor on $N(M)$. The algebraic projection of this integral divisor $(f)_{N(M)}$ on M is called the *generalized divisor* of the function f on M and is denoted by $(f)_M$ or merely by (f). If Z_0 and Z_∞ are the positive and negative parts of $(f)_{N(M)}$ respectively, then $\mathrm{pr}\,Z_0$ and $\mathrm{pr}\,Z_\infty$ are called the generalized *zero-divisor* and the generalized *pole-divisor* of f on M and they are denoted by $(f)_{0M}$ and $(f)_{\infty M}$ or merely by $(f)_0$ and $(f)_\infty$ respectively. Since $(f)_{N(M)} = Z_0 - Z_\infty$, we have $(f)_M = (f)_{0M} - (f)_{\infty M}$. Though Z_0 and Z_∞ have no common component, $(f)_{0M}$ and $(f)_{\infty M}$ may have some common components.

THEOREM 13. *Let M, f and I be as above and let I^* be a ground ring containing I. Then*

$$\begin{aligned} &\sigma_{I^*/I}((f)_M) = (f)_{M\otimes I^*}, \\ (1) \qquad &\sigma_{I^*/I}((f)_{0M}) = (f)_{0,M\otimes I^*}, \\ &\sigma_{I^*/I}((f)_{\infty M}) = (f)_{\infty,M\otimes I^*}. \end{aligned}$$

If, for any spot P of rank 1 *in M, either f or f^{-1} is in P, then*

$$\begin{aligned} &(f)_{0M} = \textstyle\sum e(fP)P \quad (\text{where } P \text{ runs over all spots of rank 1 in } M \text{ which contains } f), \\ (2) \qquad & \\ &(f)_{\infty M} = \textstyle\sum e(f^{-1}P)P \quad (\text{where } P \text{ runs over all spots of rank 1 in } M \text{ which contains } f^{-1}). \end{aligned}$$

Proof. (2) is an immediate consequence of the extension formula of multiplicity (see [3]). Applying (2) to $N(M) \otimes I^*$, we have

$$(f)_{0,N(M)\otimes I^*} = \sum e(fP^*)P^* \quad (f \in P^*, \mathrm{rank}\,P^* = 1, P^* \in N(M) \otimes I^*)$$

and

$$(f)_{\infty,N(M)\otimes I^*} = \sum e(f^{-1}P^*)P^* \quad (f^{-1} \in P^*, \mathrm{rank}\,P^* = 1, P^* \in N(M) \otimes I^*).$$

For an arbitrary spot P^* of rank 1 in $N(M)\otimes I^*$ which contains f, let P be the spot of rank 1 in $N(M)$ which is dominated by P^*. Then the coefficient c of P^* in $\sigma_{I^*/I}((f)_{N(M)})$ is equal to $v_P(f)\cdot i(P/I;P^*/I^*)$ by the definition of $\sigma_{I^*/I}$. Since P is a valuation ring, we have easily $c=\epsilon(fP^*)$ and we have $\sigma_{I^*/I}((f)_{0,N(M)})=(f)_{0,N(M)\otimes I^*}$. Similarly we have

$$\sigma_{I^*/I}((f)_{\infty,N(M)})=(f)_{\infty,N(M)\otimes I^*}.$$

Therefore (1) follows from the following

PROPOSITION 9. $\mathrm{pr}^{M'\otimes I^*}{}_{M\otimes I^*}\cdot\sigma_{I^*/I}=\sigma_{I^*/I}\cdot\mathrm{pr}^{M'}{}_M$, *where M, M', I and I^* are as above.*

Proof. It is sufficient to prove $\mathrm{pr}\cdot\sigma_{I^*/I}P'=\sigma_{I^*/I}\cdot\mathrm{pr}\,P'$ for an arbitrary spot $P'\in M'$. $\sigma_{I^*/I}P'=\sum i(P'/I;P^*{}_j/I^*)P^*{}_j$, where $P^*{}_j$ runs over all components of $P'\times I^*$. Let $\mathfrak{m}'$ be the maximal ideal of P'. Then $i(P'/I;P^*{}_j/I^*)$ $=l(P^*{}_j/\mathfrak{m}'P^*{}_j)$, hence $\mathrm{pr}\cdot\sigma_{I^*/I}P'=\sum_j l(P^*{}_j/\mathfrak{m}'P^*{}_j;\mathrm{proj}\,P^*{}_j)\,(\mathrm{proj}\,P^*{}_j)$. This shows that, if $P_1,\cdots,P_r$ are components of $\mathrm{pr}\cdot\sigma_{I^*/I}P'$, then $\mathrm{pr}\cdot\sigma_{I^*/I}P'$ $=\sum_j l((P'\times I^*)_{S(j)};P_j)P_j$, where $S(j)$ is the intersection of complements of maximal ideals in $P'\times I^*$ which lie over that of P_j. On the other hand, if we denote by P and $\mathfrak{m}$, $\mathrm{pr}\,P'$ and its maximal ideal, then

$$\begin{aligned}\sigma_{I^*/I}\cdot\mathrm{pr}\,P'&=[\phi_{P'}(P'):\phi_P(P)]\cdot(\textstyle\sum i(P/I;P_j/I^*)P_j)\\&=\textstyle\sum l(P_j/\mathfrak{m}P_j)\cdot[\phi_{P'}(P'):\phi_P(P)]\cdot P_j.\end{aligned}$$

Now we see the equality of these two generalized cycles easily.

9. Ideals on a model. An *ideal* $\mathfrak{A}$ of a model M is a set of ideals $\mathfrak{a}(P)$ of spots $P\in M$ ($\mathfrak{a}(P)$ may be equal to P) such that for any spot $P\in M$, there exists an affine model A contained in M and containing P which satisfies the following condition: There is an ideal $\mathfrak{a}$ of the affine ring $\mathfrak{o}$ of A such that $\mathfrak{a}(Q)=\mathfrak{a}Q$ for any spot $Q\in A$. $\mathfrak{a}(P)$ is called the *P-component* of $\mathfrak{A}$ and the ideal $\mathfrak{a}$ above is called the *affine representative* of $\mathfrak{A}$ in A (or in $\mathfrak{o}$).

This definition shows that for an ideal $\mathfrak{A}$ of a model M, there exist a finite number of affine models $A_1,\cdots,A_n$ such that 1) M is the union of the A_i and 2) $\mathfrak{A}$ has the affine representative in each of the A_i.

Sums, products and intersections of ideals of a model are defined by component-wise operations.

If $\mathfrak{A}$ is an ideal of a model M, the set of spots $P\in M$, such that the P-component of $\mathfrak{A}$ is different from P, forms obviously a closed set of M, which is called the *closed set* defined by the ideal $\mathfrak{A}$.

We say that an ideal in a model M is *prime* or *primary* if 1) the closed set defined by the ideal is irreducible and 2) every component is prime or primary respectively. Then we see the decomposition theorems to intersections of primary ideals as in the case of Noetherian rings.

Remark. If $\mathfrak{a}$ is an ideal of an affine ring $\mathfrak{o}$, then $\mathfrak{a}$ defines an ideal $\mathfrak{A}$ of the affine model A of $\mathfrak{o}$ such that the P-component of $\mathfrak{A}$ is $\mathfrak{a}P$ for any $P \in A$. If $\mathfrak{b}$ is a homogeneous ideal of a homogeneous coordinate ring of a projective model M, then $\mathfrak{b}$ defines an ideal $\mathfrak{B}$ of M as follows: Let $\mathfrak{h} = I[z_0, \cdots, z_n]$ be the homogeneous coordinate ring (z_i are homogeneous elements of degree 1). If a spot P is in the affine model of $I[z_0/z, \cdots, z_n/z]$ (z being a homogeneous element of degree 1), then let $\mathfrak{b}(z)$ be the set of elements of the form b/z^r with homogeneous element b of degree r (r being arbitrary). Then $\mathfrak{b}(z)$ is an ideal of $I[z_0/z, \cdots, z_n/z]$ and $\mathfrak{b}(z)P$ is uniquely determined (independently on the choice of z). Now, $\mathfrak{B}$ is defined so that the P-component is $\mathfrak{b}(z)P$.

Ideals $\mathfrak{A}$ and $\mathfrak{B}$ obtained as above are called *ordinary ideals.*

Let $\mathfrak{A}$ be an ideal of an absolutely irreducible model M and let F be the closed set defined by $\mathfrak{A}$. Let $P_1, \cdots, P_n$ be the generating spots of the irreducible components of F and let $\mathfrak{a}_i$ be the P_i-component of $\mathfrak{A}$ for each i. Then $\mathfrak{a}_i$ is a primary ideal belonging to the maximal ideal of P_i. Then $\mathfrak{A}$ defines two integral cycles $\sum l(P_i/\mathfrak{a}_iP_i)P_i$ and $\sum e(\mathfrak{a}_i)P_i$; they are denoted by $Z_1(\mathfrak{A})$ and $Z_2(\mathfrak{A})$ respectively. $\max(\operatorname{rank} P_1, \cdots, \operatorname{rank} P_n)$ and $\min(\operatorname{rank} P_1, \cdots, \operatorname{rank} P_n)$ are called *maximal rank* and *minimal rank of* $\mathfrak{A}$ respectively, and denoted by max-rank $\mathfrak{A}$ and min-rank $\mathfrak{A}$. If max-rank $\mathfrak{A}$ = min-rank $\mathfrak{A}$, then this number is called the *rank* of $\mathfrak{A}$ and is denoted by rank $\mathfrak{A}$.

If rank $\mathfrak{A}$ is defined and if every component of $\mathfrak{A}$ is generated by rank $\mathfrak{A}$ elements, then $\mathfrak{A}$ is said to be a *principal ideal* of rank (rank $\mathfrak{A}$). Observe that if $\mathfrak{A}$ is a principal ideal of rank r and if each P_i defined above has a distinct system of parameters, then $Z_1(\mathfrak{A}) = Z_2(\mathfrak{A})$. In particular, if $\mathfrak{A}$ is a principal ideal of rank 1, then $Z_1(\mathfrak{A}) = Z_2(\mathfrak{A})$, which is called the *effective principal divisor* defined by $\mathfrak{A}$. In general, if $Z_1(\mathfrak{A}) = Z_2(\mathfrak{A})$ for an ideal $\mathfrak{A}$, the integral cycle $Z_1(\mathfrak{A})$ is called the *integral cycle defined by* $\mathfrak{A}$ and is denoted by $Z(\mathfrak{A})$.

If D is an effective principal divisor (defined some principal ideal of rank 1) on a model M, then for every spot P of M there exists an affine model A contained in M and containing P such that $[D]_A = (f_A)_A$ for an element f_A of the affine ring of A. Such an f_A is called a *local equation* of D at P, or on A.

PROPOSITION 10. *If* $\mathfrak{A}_1$ *and* $\mathfrak{A}_2$ *are principal ideals of rank* 1 *on* M, *then* $\mathfrak{A}_1\mathfrak{A}_2$ *is also principal and* $Z(\mathfrak{A}_1\mathfrak{A}_2) = Z(\mathfrak{A}_1) + Z(\mathfrak{A}_2)$. *Furthermore, if* D *is an integral divisor contained in the group generated by all effective principal divisors, then for any spot* $P \in M$, *there exists an affine model* A *contained in* M *and containing* P *such that* $[D]_A = (f_A)_A$ *with a function* f_A *on* M.

Proof. Easy.

f_A as above is called the *local equation* of D at P, or on A. The group generated by all effective principal divisors is called the *principal divisor group*, and elements of the group are called *principal divisors.*

On the other hand, let I^* be a ground ring containing I. Then for an ideal $\mathfrak{A}$ of M, the ideal $\mathfrak{A}^*$ of $M \otimes I^*$ defined as follows is called the *extension* of $\mathfrak{A}$ over I^*, or in $M \otimes I^*$, and is denoted by $\mathfrak{A} \otimes I^*$: For an arbitrary spot $P^* \in M \otimes I^*$, let P be the spot in M which is dominated by P^* (i.e., P^* is an extension of P), and let $\mathfrak{a}(P)$ be the P-component of $\mathfrak{A}$. Then the P^*-component of $\mathfrak{A}^*$ is defined to be $\mathfrak{a}(P)P^*$. More generally, if M' is a model dominating M, then we define the *extension* of $\mathfrak{A}$ in M' by the same way. By our definition, we see easily the following

THEOREM 14. $\sigma_{I^*/I}(Z_i(\mathfrak{A})) = Z_i(\mathfrak{A} \otimes I^*)$ *for* $i = 1, 2$,

Proof. As for $i = 1$, the proof is easy. Since $\sigma_{I^*/I}(Z_1(\mathfrak{A}^n)) = Z_1(\mathfrak{A}^n \otimes I^*)$ for any $n = 1, 2, 3, \cdots$, we see the equality in the case where $i = 2$.

10. Linear equivalence classes of divisors and line bundles. We say that two generalized divisors D and D' on a model M are *linearly equivalent* to each other if there exists a function f on M such that $D - D' = (f)$; in this case, we write $D \sim D'$.

PROPOSITION 11. *If* I *is a Dedekind domain and if* u *is a transcendental element over* I, *then* $I(u)$ *is a unique factorization ring.*

Proof. Let $\mathfrak{p}^*$ be any prime ideal of rank 1 in $I(u)$ and set $\mathfrak{p} = I \cap \mathfrak{p}^*$. Then we have $\mathfrak{p}^* = \mathfrak{p}I(u)$. Since I is a Dedekind domain, $\mathfrak{p}$ is generated by two elements, say, a and b. Set $x = au + b$. Then we see that $\mathfrak{p}^*$ is the unique prime ideal of $I(u)$ containing x and that $xI(u)_{\mathfrak{p}^*} = \mathfrak{p}I(u)_{\mathfrak{p}^*} = \mathfrak{p}^*I(u)_{\mathfrak{p}^*}$, which shows that $xI(u) = \mathfrak{p}^*I(u)$. Therefore $I(u)$ is a unique factorization ring.

THEOREM 15. *Let D be a principal divisor on a model M of a function field L over a ground ring I and let I^* be a canonical extension of I (with respect to a universal domain).*

(1) *If there exists a function f on $M\otimes I^*$ such that $(f)_{M\otimes I^*} \succ \sigma_{I^*/I}(D)$, then f can be expressed in the form $\sum_1^n c_i w_i$ with $c_i \in I^*$ and $w_i \in L$ such that $(w_i)_M \succ D$ for each i.*

(2) *if there exists a function f on $M\otimes I^*$ such that $(f)_{M\otimes I^*} = \sigma_{I^*/I}(D)$ and if M is complete, then there exists a function g on M such that* (i) *$g/f \in I^*$ and* (ii) *$(g)_M - D$ is an effective principal divisor with local equations in I.*

(3) *Besides the conditions in* (2), *if I is a unique factorization ring, then we can choose g so that $(g)_M = D$, namely, D is linearly equivalent to zero on M.*

Proof. We shall prove (1) first. We may assume that I^* is finitely generated over I, namely, there are a finite number of algebraically independent elements $u_1,\cdots,u_n$ over I such that I^* is a finite integral extension of $I(u_1,\cdots,u_n)$. We shall use induction on n. Assume that $n \geqq 1$. Then set $I' = I(u_1)$, $D' = {}_{I'/I}(D)$. Then by induction on $n \cdot f = \sum c_i w'_i$ with $c_i \in I^*$ and $w'_i \in L(u_1)$ such that $(w'_i)_{M\otimes I'} \succ D'$. Therefore if we know that the assertion is true for the cases where $n = 0$ and $I^* = I(u)$ with a transcendental element u, then we see that the assertion is true in every case. Thus we shall consider only these cases. We shall show at first that $f \in L\otimes I^*$. This is obvious if I^* is integral over I and therefore we assume that $I^* = I(u)$. Since $L[u]$ is a unique factorization ring, we see that $L\otimes I^*$ is a unique factorization ring. Therefore we see easily that if f is not in $L\otimes I^*$, then there exists a simple spot P^* of rank 1 in $M\otimes I^*$ such that (i) $L\otimes I^* \subseteq P^*$ and (ii) f^{-1} is a non-unit in P^*. Then the negative component of (f) has P^* as a component and we have a contradiction to the assumption that $(f) \succ \sigma_{I^*/I}(D)$. Thus $f \in L\otimes I^*$. Let $A_1,\cdots,A_m$ be affine models contained in M such that M is the union of the A_i and that D has a local equation f_i on A_i for each i. If P is an arbitrary spot of rank 1 in A_i, then f/f_i is in every component of $P\times I^*$ and therefore $f/f_i \in P\otimes I^*$ by Theorem 2. Therefore there are a finite number of elements $c_1,\cdots,c_r$ of I^* such that $f/f_i \in P\otimes(\sum Ic_j)$ for any i and P. Since I is a Dedekind domain, there is a module $\mathfrak{M}$ such that $\mathfrak{M} + \sum Ic_j$ (direct sum) is a free module over I. Let $e_1 + m_1,\cdots,e_s + m_s$ ($e_i \in \sum Ic_j, m_i \in \mathfrak{M}$) be a linearly independent base of the direct sum. Then f is expressed uniquely in the form $\sum_1^s w_i(e_i + m_i)$ with $w_i \in L$ and that $f/f_i \in P\otimes((\sum Ic_j) + \mathfrak{M})$ shows that $w_i/f_i \in P$. There-

fore for every w_i which is not zero, we have $(w_i)_M \succ D$. Thus (1) is proved. Now we shall prove (2). By virtue of (1), there exists an element g of L such that $(g)_M \succ D$. It follows that $(g/f)_{M\otimes I^*} \succ 0$. Since M is complete, $M \otimes I^*$ is also complete, hence $g/f \in I^*$. Since $(g/f)_{M\otimes I^*} = \sigma_{I^*/I}((g)_M - D)$, the remaining part of (2) follows easily from (3), considering local models attached to ground places. Therefore we shall prove (3) lastly. Since $I(u_1, \cdots, u_n)$ is also a unique factorization ring (for algebraically independent elements u_i), we can reduce to the case where I^* is either a finite integral extension of I or of the form $I(u)$, using induction as in the proof of (1). On the other hand, by the proof of (2) above, we may assume that $f \in I^*$. Let g be a generator of $fI^* \cap I$. It is sufficient to prove that $fI^* = gI^*$. This is easy if $I^* = I(u)$ and therefore we assume that I^* is an integral extension of I. Now, in the proof of (1), since I^* is a free module over I, if we take a linearly independent base $c_1, \cdots, c_r$ of I^* over I, we see that $f = \sum c_i w_i$ with $w_i \in L$ such that $(w_i) \succ D$ for any $w_i \neq 0$. Since the w_i are unique and since $f \in I^*$, we have $w_i \in I$ and therefore $fI^* = \sum w_i I^*$ and therefore g is a generator of $\sum w_i I$ and $fI^* = gI^*$. Thus the proof of Theorem 15 is completed.

We say that a fibre bundle W with base M and fibre F is a *line bundle* if (1) F is the affine model of $I[x]$ (I is the ground ring of M, x is a transcendental element over I), which is called a model of the affine 1-space over I (see Chapter 6, § 1) and (2) for the x above, every transition mapping σ has the property that $\sigma(x)/x$ is in the function field of M.

Now let G_1 be the principal divisor group of a model M of a function field L over a ground ring I. The set of general divisors which are linearly equivalent to zero form a subgroup of G_1, which will be denoted by G_2 in this section.

Let D be an element of G_1. Then there are affine models $A_1, \cdots, A_n$ such that 1) the union of the A_i is M and 2) D has a local equation f_i on each A_i. Then f_i/f_j is a unit in $A_i \cap A_j$. Let x be a variable over L and let σ_i be the automorphism of $L(x)$ such that $\sigma_i(x) = f_i x$. Then defining σ_i to be the transition mapping on A_i, we have a line bundle, which is called a *line bundle defined by* D and is denoted by $W(D)$. It is easy to see that $W(D)$ is unique to within equivalence of line bundles.

THEOREM 16. *Let D and D' be elements of G_1 above. Then $W(D)$ and $W(D')$ are equivalent to each other if and only if D and D' are linearly equivalent to each other. Furthermore, any line bundle is equivalent to some $W(D)$ $(D \in G_1)$ and therefore there is a one to one correspondence between G_1/G_2 and the set of equivalence classes of line bundles.*

Proof. If D and D' are linearly equivalent to each other, then there exists an element f of L such that $D - D' = (f)$. Therefore when g_i's are local equations for D', fg_i's are local equations for D and we see the equivalence between $W(D)$ and $W(D')$. Conversely, assume that $W(D)$ and $W(D')$ are equivalent to each other. Let $A_1, \cdots, A_n$ be affine models such that $M = \cup_i A_i$ and D and D' have local equations g_i and g'_i on each A_i. We may assume that $W(D)$ and $W(D')$ are defined by these local equations. Since $W(D)$ and $W(D')$ are equivalent to each other, there exists an automorphism σ of $L(x)$ over L such that $\sigma W(D) = W(D')$. Let F be the affine model of $I[x]$. Since σ is an automorphism over L, it follows that $\sigma\sigma_i(A \otimes F) = \sigma'_i(A_i \otimes F)$, where σ_i and σ'_i are transition mappings of $W(D)$ and $W(D')$ respectively $(\sigma_i(x) = g_i x, \sigma'_i(x) = g'_i x)$. Let $\mathfrak{o}_i$ be the affine ring of A_i. Then we have $\mathfrak{o}_i[\sigma\sigma_i(x)] = \mathfrak{o}_i[\sigma'_i(x)]$, i.e., if a and b are elements of L such that $\sigma(x) = ax + b$, then $\mathfrak{o}_i[ag_i x + bg_i] = \mathfrak{o}_i[g'_i x]$. Then we have $g_i b \in \mathfrak{o}_i$ and ag_i/g'_i is a unit in $\mathfrak{o}_i$. Therefore ag_i is also a local equation of D' on A_i and $D' - D = (a)$. Thus D is linearly equivalent to D'. Now, let W be an arbitrary line bundle with base M and fibre F defined by $I[x]$. Let $A_1, \cdots, A_n$ and transition mappings $\sigma_1, \cdots, \sigma_n$ be as in the definition of line bundles. Since $\sigma_i(x) = g_i x$ with $g_i \in L$ and since g_i/g_j is a unit in every spot in $A_i \cap A_j$, there is a member of G_1 which has the g_i as local equations on the A_i, say D. Then $W = W(D)$. Thus the proof is completed.

Chapter 6. Simple Spots.

1. The set of simple spots in a model. A model M is called a *non-singular model* if every spot in M is a simple spot; it is called an *unramified non-singular model* if every spot in M is an unramified simple spot.

Remark 1. Though the notion of non-singular model does not depend on the choice of ground ring, the notion of unramified non-singular model depends on the choice of ground ring. If the ground ring is a field, then these two notions coincide to each other.

An affine model A is called a model of the *affine n-space* over a ground ring I if the affine ring of A is isomorphic to the polynomial ring in n algebraically independent elements over I (and if it is regarded as a model over I). A projective model M over I is called a model of the *projective n-space* if it is defined by a homogeneous coordinate system $(z_0, \cdots, z_n)$ with $n+1$ algebraically independent elements z_i. The dimension of these models

is either n or $n+1$ according to whether I is a field or not. A model of the projective n-space is the union of $n+1$ models of affine n-space.

Remark 2. Any affine (or projective) model can be regarded as an induced model of a model of affine (or projective) n-space for some n.

PROPOSITION 1. *If M is a model of affine or projective n-space, then M is an unramified non-singular absolutely irreducible model.*

Proof. This follows immediately from Corollary 5 to Proposition 1.1 and its proof.

LEMMA 1. *If a function field L over a ground ring I is separably generated over I, then any model M of L contains an unramified non-singular model (over I).*

Proof. We have only to show that there exists an unramified non-singular model of L; for if it is done, then the intersection of the model with M is a model by Theorem 2.10 and is an unramified non-singular model. Now, let $x_1, \cdots, x_n$ be a separating transcendence base of L over I and let $b \in L$ be such that $\mathfrak{o} = I[x_1, \cdots, x_n, b]$ is an affine ring of L and such that b is integral over $I[x_1, \cdots, x_n]$. Let d be the discriminant of the irreducible monic polynomial over $I[x_1, \cdots, x_n]$ which has b as a root. Set $\mathfrak{o}' = \mathfrak{o}[1/d]$. We shall show that the affine model A defined by $\mathfrak{o}'$ is an unramified non-singular model. Let P be any spot in A. Then P dominates a spot P^* in the affine model A^* defined by $I[x_1, \cdots, x_n]$. P^* is an unramified simple spot by Proposition 1. By our construction, P is a ring of quotients of $P^*[b]$ with respect to a maximal ideal. Since d is a unit in $\mathfrak{o}'$, d is a unit in P^* and therefore P is an unramified simple spot by Proposition 3.2. Thus A is an unramified non-singular model, which proves Lemma 1.

Remark 3. There are models over some ground ring, say I, which does not contain any unramified non-singular model over I.

Example. Let k be a field of characteristic $p \neq 0$ which contains infinitely many elements and let x be a transcendental element over k. Set $I = k[x^p]$ and $\mathfrak{o} = k[x]$. Then $\mathfrak{o}$ is an affine ring over I. I contains infinitely many prime ideals of the form $(x^p - a^p)I$ $(a \in k)$ and these prime ideals ramify in $\mathfrak{o}$. Therefore the affine model A defined by $\mathfrak{o}$ contains infinitely many ramified simple spots over I. Since $\dim A = 1$, this shows that A cannot contain any unramified non-singular model over I.

LEMMA 2. *Any model contains a non-singular model.*

Proof. By the same reason as in the proof of Lemma 1, we have only to prove that any function field L over a ground ring I has a non-singular model. Let p be the characteristic of I. If $p=0$, L is separably generated over I, and the assertion is true by Lemma 1. Therefore we assume that $p\neq 0$. Let $a_1,\cdots,a_n$ be elements of some integral extension of I such that 1) $a_i p \in I[a_1,\cdots,a_{i-1}]$ for every $i=1,\cdots,n$ and 2) $L(a_1,\cdots,a_n)$ is separably generated over $I[a_1,\cdots,a_n]$. We shall prove the assertion by induction on n. If $n=0$, then L is separably generated and the case was settled by Lemma 1. Assume that $n\geqq 1$ and let I^* be the derived normal ring of $I[a_1]$. Then by our induction assumption, there exists a non-singular model M^* of $L(a_1)$ over I^*. Since I^* is a finite I-module, we may regard M^* as a model over I. Let $\mathfrak{o}$ be an affine ring of L and set $\mathfrak{o}'=\mathfrak{o}[a_1]$. Let M and M' be the affine models defined by $\mathfrak{o}$ and $\mathfrak{o}'$ respectively. Then, since a_1 is purely inseparable, the projection from M' into M is a one-one and onto mapping; if $\mathrm{proj}\, P'=P$, then $P'=P[a_1]$. Since M^* is a non-singular model of $L(a_1)$, $M^*\cap M'$ is a non-singular model of $L(a_1)$. Therefore there exists an element f of $\mathfrak{o}'$ such that the model A' defined by $\mathfrak{o}'[1/f]$ is a non-singular model. By Corollary 1 to Proposition 4.1, every spot in $\mathrm{proj}_M A'$ is a simple spot. Since $\mathrm{proj}\, A'$ is obviously the affine model defined by $\mathfrak{o}[1/f^p]$, the assertion is proved.

PROPOSITION 2. *Let P be a simple spot in a model M and let $x_1,\cdots,x_r$ be a regular system of parameters of P. Then the induced model $\phi_P(M)$ contains a model M' such that if a spot $\phi_P(Q)$ $(Q\in M(P))$ is in M', then Q is a simple spot and has a regular system of parameters which contains $x_1,\cdots,x_r$ as a subset.*

Proof. We may assume without loss of generality that M is an affine model. Let $\mathfrak{o}$ be the affine ring of M and let $\mathfrak{p}$ be the prime ideal of $\mathfrak{o}$ such that $P=\mathfrak{o}_{\mathfrak{p}}$. Furthermore, let $\mathfrak{a}$ be the ideal generated by $x_1,\cdots,x_r$ in $\mathfrak{o}$. Since $\mathfrak{a}P=\mathfrak{p}P$, $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$ and the primary component of $\mathfrak{a}$ belonging to $\mathfrak{p}$ is just $\mathfrak{p}$. Let f be an element of $\mathfrak{o}$ such that f is not in $\mathfrak{p}$ and is in every prime divisor of $\mathfrak{a}$ except for $\mathfrak{p}$. Then we may consider the affine model defined by $\mathfrak{o}[1/f]$ instead of M. Thus we may assume that $\mathfrak{a}=\mathfrak{p}$. Let M' be a non-singular model contained in $\phi_P(M)$; existence follows from Lemma 2. Let Q be any spot in $M(P)$ such that $\phi_P(Q)\in M'$. Then since $\mathfrak{a}=\mathfrak{p}$, $\phi_P(Q)=Q/\mathfrak{a}Q$. Therefore, that $\phi_P(Q)$ is simple shows that Q is also simple and that $x_1,\cdots,x_r$ are contained in a regular system of parameters of Q (Lemma 0.12). Thus the proof is completed.

Remark 4. In the above proposition, (i) if P is an unramified simple spot and if P dominates a ground place which is not a field, then any Q obtained by the proof above is also an unramified simple spot, for a prime element of the ground place dominated by P can be a member of a regular system of parameters of P; (ii) if P contains a field of quotients of I and if M' is an unramified non-singular model over I, then Q is an unramified simple spot.

By virtue of Theorem 2.9, Proposition 2.6 can be stated as follows:

PROPOSITION 3. *Let M be a model. Then a subset M' of M is a model if and only if the following conditions are satisfied:*

1) *M' is not empty.* 2) *If a spot $P \in M$ is not in M', then any specialization of P in M is not in M'.* 3) *If a spot $P \in M$ is in M', then $\phi_P(M(P) \cap M')$ contains a model.*

THEOREM 1. *The set M' of simple spots in a model M is also a model.*

Proof. We shall make use of Proposition 3. The condition 1) is obvious. Thetorem 4.1 shows the validity of the condition 2). Proposition 2 shows the validity of 3). Thus M' is a model.

PROPOSITION 4. *Let M be a model of a function field L over a ground ring I. Then the set M' of unramified simple spots in M is a model (over I) if at least one of the following conditions are satisfied:* 1) *I is a semi-local ring (or a field).* 2) *I is of characteristic zero.*

Proof. M' is obviously non-empty. Theorem 4.2 shows that if $P \in M$ is not in M', then any specialization of P is not in M'. Assume that $P \in M'$. If P dominates a ground place I' which is not a field, then Proposition 2 and Remark 4 shows the validity of Condition 3) in Proposition 3. Assume that P contains the field of quotients k of I. i) In the case 1), the set of spots in $\phi_P(M)$ which contains k contains a model and therefore $\phi_P(M(P) \cap M')$ contains a model by Remark 4. ii) In the case 2), since $\phi_P(P)$ is separably generated over I, $\phi_P(M(P) \cap M')$ contains a model by Lemma 1 and Remark 4. Therefore, by Proposition 3, we prove Proposition 4.

2. Criteria for unramified simple spots. Let $X_1, \cdots, X_n$ be algebraically independent elements over an integral domain I and let $f_1, \cdots, f_r$ be elements of $I[X_1, \cdots, X_n]$. Then the Jacobian matrix $(\partial f_i/\partial X_j)$ will be denoted by $J(f_1, \cdots, f_r)$. Let I^* be a subring of I. Then the set $\mathfrak{D}_{I/I^*}$ of integral derivations of I over I^* is an I-module. Let $\{D_\sigma\}$ be a set of

generators of $\mathfrak{D}_{I/I^*}$. Then the matrix $(\partial f_i/\partial X_j; f_i^{D\sigma})$ is called a *mixed Jacobian matrix* of $f_1, \cdots, f_r$ with respect to I^* and is denoted by $J^*(f_1, \cdots, f_r; I^*)$. Observe that $J^*(f_1, \cdots, f_r; I^*)$ is substantially unique, i.e., change of the generators of $\mathfrak{D}_{I/I^*}$ corresponds to a linear transformation of columns. Observe also that $J(f_1, \cdots, f_r) = J^*(f_1, \cdots, f_r; I)$.

THEOREM 2. *Assume that $I = k$ is a field and set $A = k[X_1, \cdots, X_n]$. Let $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals of A and set $R = A_{\mathfrak{q}}$. Furthermore, let $\mathfrak{a} = \sum_1^r f_i A$ be an ideal having $\mathfrak{p}$ as a prime divisor. Then:*

(1) *If $A/\mathfrak{q}$ is separably generated over k, $R/\mathfrak{a}R$ is a simple spot if and only if rank $(J(f_1, \cdots, f_r)$ modulo $\mathfrak{q}) =$ rank $\mathfrak{p}$.*

(2) *If k is of characteristic $p \neq 0$, then $R/\mathfrak{a}R$ is a simple spot if and only if there exists a subfield k^* of k such that $[k : k^*]$ is finite and such that rank $(J^*(f_1, \cdots, f_r; k^*)$ modulo $\mathfrak{q}) =$ rank $\mathfrak{p}$; or equivalently, rank$(J^*(f_1, \cdots, f_r; k^p)$ modulo $\mathfrak{q}) =$ rank $\mathfrak{p}$.*

For the proof, see Nagata [4] or Zariski [8].

It should be remarked here that when $\mathfrak{p}$ is a prime ideal of $I[X_1, \cdots, X_n]$, $\mathfrak{p} = \sum_1^r f_i I[X_1, \cdots, X_n]$, that rank$(J(f_1, \cdots, f_r)) =$ rank $\mathfrak{p}$ means that 1) $\mathfrak{p} \cap I = 0$ and 2) $I[X_1, \cdots, X_n]/\mathfrak{p}$ is separably generated over I.

As for the case of spots over a ground ring, we have the following application of Theorem 2:

Assume that I is a ground ring, $\mathfrak{o} = I[X_1, \cdots, X_n]$, $\mathfrak{p} \subseteq \mathfrak{q}$ are prime ideals of $\mathfrak{o}$, $\mathfrak{a} = \sum_1^r f_i \mathfrak{o}$ is an ideal having $\mathfrak{p}$ as a prime divisor and that $\mathfrak{p} \cap I = 0$. Set $R = \mathfrak{o}_{\mathfrak{q}}$. Then

THEOREM 3. *If rank $(J(f_1, \cdots, f_r)$ modulo $\mathfrak{q}) =$ rank $\mathfrak{p}$, then $R/\mathfrak{a}R$ is an unramified simple spot. Conversely, if $R/\mathfrak{a}R$ is a tamely unramified simple spot, then rank $(J(f_1, \cdots, f_r)$ modulo $\mathfrak{q}) =$* rank $\mathfrak{p}$.

Proof. If the field of quotients of I is contained in $R/\mathfrak{a}R$ (*i.e.*, $\mathfrak{q} \cap I = 0$), then the assertion is contained in Theorem 2. Therefore we assume that I is not a field and is a ground place dominated by R. Let p be a prime element of I $(p \in \mathfrak{q})$. If rank $(J(f_1, \cdots, f_r)$ modulo $\mathfrak{q}) =$ rank $\mathfrak{p}$, then we have $R/(pR + \mathfrak{a}R)$ is a simple spot over I/pI. Therefore $(pR + \mathfrak{a}R)/\mathfrak{a}R \supseteq \mathfrak{p}R/\mathfrak{a}R$, and $\mathfrak{p}R = \mathfrak{a}R$ and therefore $R/\mathfrak{a}R$ is an unramified simple spot over I. Conversely, if $R/\mathfrak{a}R$ is a tamely unramified simple spot, then $R/(pR + \mathfrak{a}R)$ is a tamely unramified simple spot over I/pI, hence rank $(J(f_1, \cdots, f_r)$ modulo $\mathfrak{q}) =$ rank $\mathfrak{p}$.

COROLLARY. *If a model M over a ground ring I carries a tamely unramified simple spot, then the function field of M is separably generated over I.*

Remark. The second criterion in Theorem 2 can be applied for unramified simple spots. But it depends on the ground place dominated by the spot (apply the criterion in the case where k is the residue class field of the ground place).

We shall give here a remark on projective models.

Let M be a projective model of a function field L over a ground ring I and let $\mathfrak{H}=I[z_0,\cdots,z_n]$ be a homogeneous coordinate ring which defines M. Then $\mathfrak{H}$ is an affine ring of $L(z_i)$ with some $z_i\neq 0$ and such z_i is a transcendental element over L.

Now let P be a spot in M. Then there exists a uniquely determined prime ideal $\mathfrak{p}$ of $\mathfrak{H}$ such that if $z_i\notin\mathfrak{p}$ then a homogeneous form $f\in\mathfrak{H}$ is in $\mathfrak{p}$ if and only if f/z_i^d ($d=\deg f$) is in the maximal ideal of P and $\mathfrak{H}/\mathfrak{p}$ is a homogeneous coordinate ring of the induced model $\phi_P(M)$. Then obviously $\mathfrak{H}_\mathfrak{p}$ dominates P. Since $\mathfrak{H}/\mathfrak{p}$ is a homogeneous coordinate ring of $\phi_P(M)$, we see that $\mathfrak{H}_\mathfrak{p}=P(z_i)$ with some $z_i\notin\mathfrak{p}$.

By virtue of this fact, it is sometimes convenient to consider the affine model M^* defined by $\mathfrak{H}$, which is called the model of a representative cone of M. For example, P is a simple spot (or a normal spot) if and only if the corresponding spot $\mathfrak{H}_\mathfrak{p}$ is simple (or normal, respectively). Thus, we can apply the Jacobian criterion for simple spots in M, using the homogeneous coordinate ring $\mathfrak{H}$, namely:

Let $\mathfrak{o}$ be the polynomial ring in indeterminates $Z_0,\cdots,Z_n$ over I and let $\mathfrak{P}$ be the kernel of the homomorphism ϕ from $\mathfrak{o}$ onto $\mathfrak{H}$ such that $\phi(Z_i)=z_i$. Let $f_1,\cdots,f_r$ be a set of generators of $\mathfrak{P}$. Then we get a criterion for simplicity of spots in M, quite similar to the assertion in Theorem 3, using $J(f_1,\cdots,f_r)$.

3. Absolutely simple spots. A spot P is called *absolutely simple* if 1) P is a regular extension of the ground ring I and 2) for any ground ring I^* containing I, any extension of P over I^* is a simple spot.

A model M over a ground ring I is said to be *absolutely non-singular* if every spot in M is absolutely simple. For example, a model of the affine (or projective) n-space is absolutely non-singular.

THEOREM 4. *An absolutely simple spot is an unramified simple spot.*

Proof. Let P be an absolutely simple spot over a ground ring I. Assume

that P is ramified. We may assume that I is a valuation ring with a prime element x. Then x is in the square of the maximal ideal $\mathfrak{m}$ of P. Let $y_1, \cdots, y_r$ be a regular system of parameters of P. Set $I' = I[a]$ with $a^2 = x$. Then I' is a valuation ring. The extension P^* of P over I' is $P[a]$. Since, by assumption, $P[a]$ is a simple spot, and since the maximal ideal $\mathfrak{m}^*$ of P^* is generated by $a, y_1, \cdots, y_r$, there is a non-trivial relation $ac_0 + \sum_1^r y_i c_i = a\sum_1^r y_i d_i + \sum_{ij} y_i y_j e_{ij}$ with $c_i, d_i, e_{ij} \in P$ and $c_j = 0$ if $c_j \in \mathfrak{m}$. Since $1, a$ are linearly independent over P, we have $c_0 = \sum y_i d_i$, $\sum y_i c_i \in \mathfrak{m}^2$, hence all c_i must be zero, which is a contradiction. Thus we prove Theorem 4.

THEOREM 5. *With the same notations as in Theorem 3, $R/\mathfrak{a}R$ is an absolutely simple spot if and only if* 1) *it is a regular extension of I and* 2) *rank* $(J(f_1, \cdots, f_r)$ *modulo* $\mathfrak{q}) =$ *rank* $\mathfrak{p}$.

Proof. The conditions are independent of ground ring extensions. Therefore Theorem 5 follows easily from Theorems 3 and 4.

COROLLARY 1. *Let M be an absolutely irreducible model over a ground ring I. Then the set M' of absolutely simple spots forms a model (over I).*

Proof. Let A be an arbitrary affine model contained in M and let $\mathfrak{s}$ be the affine ring of A. Then there exists a polynomial ring $\mathfrak{o} = I[X_1, \cdots, X_n]$ such that $\mathfrak{s} = \mathfrak{o}/\mathfrak{p}$ with a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$. Let $f_1, \cdots, f_r$ be a set of generators of $\mathfrak{p}$ and let $d_1, \cdots, d_s$ be the set of subdeterminants of degree $=$ rank $\mathfrak{p}$, of the Jacobian matrix $J(f_1, \cdots, f_r)$. Let $\mathfrak{b}$ be the ideal of $\mathfrak{s}$ generated by the residue classes of the d_i modulo $\mathfrak{p}$. Then Theorem 5 shows that $A \cap (M - M')$ is a closed set of A defined by the ideal $\mathfrak{b}$. Therefore $A \cap (M - M')$ is a closed set for any affine model A contained in M, which shows that $M - M'$ is a closed set by Theorem 2.8, hence M' is a open set of M. Since M' is not empty (for example, the function field L of M is in M'), we see that M' is a model over I by Theorem 2.9.

COROLLARY 2. *A tamely unramified simple spot over a ground ring I is an absolutely simple spot if it is a regular extension of I.*

Remark. Zariski [8] defined absolutely simplicity without the assumption of regularity of the extension: In his sense, a spot P over a ground field k is absolutely simple if for any extension field k^* of k and for any prime ideal $\mathfrak{n}$ of $P \otimes k^*$ containing the maximal ideal of P, $(P \otimes k^*)_\mathfrak{n}$ is a simple spot over k^* (the condition is equivalent even if we restrict k^* to algebraic extensions of k). Under this definition, absolute simplicity is characterized by the condition 2) in Theorem 5. But, if the same definition is applied to

spots over ground rings, then, as is easily seen, Theorem 4 becomes false (for instance, let I' be a valuation ring which is finite separable and ramified extension of a ground place I and let P be an absolutely simple spot in our sense which dominates I'. If we regard P as a spot over I, then P becomes an absolutely simple spot in the sense of Zariski and is ramified over I). Therefore the condition 2) in Theorem 5 is not a necessary condition for absolute simplicity in this weak sense.

4. The set of absolutely normal spots.

THEOREM 6. *Let M be an absolutely irreducible model over a ground ring I. Then the set M' of absolutely normal spots in M forms a model over I.*

Proof. 1) When I is a field, let I^* be the smallest perfect field containing I. Then Theorem 5.9 shows that the set of spots in $M \otimes I^*$ which are absolutely normal is the set $M' \otimes I^*$ of spots in $M \otimes I^*$ which are extensions of spots in M'. Since I^* is perfect, $M' \otimes I^*$ is nothing but the set of normal spots in $M \otimes I^*$ by Corollary 2 to Theorem 5.6, hence it is a model. Now, observing the natural one-one correspondence between spots in M and $M \otimes I^*$, we see easily that M' is an open set of M, hence M' is a model because it is non-empty.

2) Now we consider the case where I is not a field. Let k be the field of quotients of I. Lemma 5.4.1 shows that $P \in M$ is absolutely normal if and only if i) any spot which is a ring of quotients of $P[k]$ is absolutely normal and ii) if $P(\mathfrak{p})$ is a general spot over a prime ideal $\mathfrak{p}$ of I and if P is a specialization of $P(\mathfrak{p})$ then $P(\mathfrak{p})$ is absolutely normal. The absolute normality of $P(\mathfrak{p})$ is equivalent to the absolute simplicity of $P(\mathfrak{p})$. Since the set of absolutely simple spots in M forms a model by Corollary 1 to Theorem 5, there exists only a finite number of general spots over some prime ideals of I which are not absolutely simple: Let them be $P_1, \cdots, P_n$. Then M' is contained in $M - (\cup_i M(P_i))$. Therefore, considering $M - (\cup_i M(P_i))$, we may assume that all the $P(\mathfrak{p})$ are absolutely simple. Let M^* be the restricted model of M over k. Then by 1), the complement of $M^* \cap M'$ in M^* is a closed set of M^*, hence there are a finite number of spots $Q_1, \cdots, Q_m$ in M^* such that the closed set if the union of the $M^*(Q_i)$. Now, Lemma 5.4.1, quoted above, shows that $M' = M - (\cup_i M(Q_i))$, which proves Theorem 6.

5. Simple points. We shall use the same notations as in § 5, Chapter 5. Then

THEOREM 7. *The following three conditions are equivalent to each other:*

(1) *The point P in the variety M' is a simple point.*

(2) *Every P_σ is absolutely simple.*

(3) *There exists one I_σ such that P_σ is absolutely simple.*

Proof. Assume that (1) is true. Then considering I_σ such that $\phi_P(P_\sigma)$ is separably generated over $\phi_P(I_\sigma)$, we see that (3) is true by Theorems 3 and 5. Since the Jacobian matrix is independent of I_σ, we see that (2) follows from (3). It is obvious that (1) follows from (2). Therefore Theorem 7 is proved.

We remark that Corollary 1 to Theorem 5 and Theorem 6 show respectively that the set of simple points and the set of normal points form open sets of the variety M' in I-topology.

6. Tensor products of simple spots.

THEOREM 8. *Let P and P' be simple spots which dominates the same ground place I.*

(1) *If $\phi_P(P) \otimes_{\phi_P(I)} \phi_{P'}(P')$ has no nilpotent element (other than zero) and if P is unramified, then for any prime ideal $\mathfrak{p}$ of $P \times_I P'$, $(P \times P')_{\mathfrak{p}}$ is a simple spot over I.*

(2) *If P and P' are unramified, then for any prime ideal $\mathfrak{p}$ of $P \otimes_I P'$, $(P \otimes P')_{\mathfrak{p}}$ is an unramified simple spot over I.*

Proof. (1) Let $\mathfrak{m}$ and $\mathfrak{m}'$ be the maximal ideals of P and P' respectively. By our assumption, the ideal $\mathfrak{a}$ generated by $\mathfrak{m}$ and $\mathfrak{m}'$ in $P \times P'$ is semi-prime. If $\mathfrak{n}$ is a maximal ideal of $P \times P'$, then $\mathfrak{n}(P \times P')_{\mathfrak{n}}$ is generated by $\mathfrak{a}$. i) When I is a field, rank $(P \times P')_{\mathfrak{n}} = \operatorname{rank} P + \operatorname{rank} P'$ and we see that $(P \times P')_{\mathfrak{n}}$ is a simple spot. ii) If I is a valuation ring having a prime element x, considering a regular system of parameters of P which has x as a member, we see that $(P \times P')_{\mathfrak{n}}$ is a simple spot. Now we see that $(P \times P')_{\mathfrak{p}}$ is a simple spot by Theorem 4.1.

(2) If I is a field, we see the validity of (2) by the criterion of simplicity by mixed Jacobian matrix as follows: Let $I[X_1, \cdots, X_m]$ and $I[Y_1, \cdots, Y_n]$ be polynomial rings in indeterminates X_i and Y_j such that $P = I[X_1, \cdots, X_m]_{\mathfrak{M}}/(f_1, \cdots, f_r)$, $P' = I[Y_1, \cdots, Y_n]_{\mathfrak{M}'}/(g_1, \cdots, g_s)$ with prime ideals $\mathfrak{M}$ and $\mathfrak{M}'$ and elements f_i and g_j. Let $\mathfrak{P}$ be the prime ideal of $I[X_1, \cdots, X_m, Y_1, \cdots, Y_n]$ such that

$$(P \otimes P')_{\mathfrak{p}} = I[X_1, \cdots, X_m, Y_1, \cdots, Y_n]_{\mathfrak{P}}/(f_1, \cdots, f_r, g_1, \cdots, g_s).$$

Since rank $(J^*(f_1, \cdots, f_s; I^p)$ modulo $\mathfrak{M}) =$ rank $(f_1, \cdots, f_r)$ and

$$\text{rank } (J^*(g_1, \cdots, g_s; I^p) \text{ modulo } \mathfrak{M}') = \text{rank } (g_1, \cdots, g_s),$$

we have

$$\text{rank } (J^*(f_1, \cdots, f_r, g_1, \cdots, g_s; I^p) \text{ modulo } \mathfrak{P}) = \text{rank } (f_1, \cdots, f_r, g_1, \cdots, g_s),$$

which proves the simplicity of $(P \otimes P')_{\mathfrak{p}}$ (since I is a field, it is unramified). If I is a valuation ring, let x be a prime element of I. Then by the case where I is a field, $(P \otimes P')_{\mathfrak{p}}/(x)$ is a simple spot over I/xI, hence $(P \otimes P')_{\mathfrak{p}}$ is an unramified simple spot.

COROLLARY. *If M and M' are absolutely non-singular models over the same ground ring I, then $M \otimes M'$ is also absolutely non-singular and conversely. If M and M' are unramified non-singular models over I and if $M \otimes M'$ is well defined, then $M \otimes M'$ is also unramified non-singular and conversely.*

Proof. The last half follows from Theorem 8 and its proof, while the first half can be proved by the same way using Jacobian matrices.

HARVARD UNIVERSITY AND KYOTO UNIVERSITY.

REFERENCES.

[1] M. Nagata, "Basic theorems on general commutative rings," *Memoirs of the College of Science, University of Kyoto*, Ser. A, vol. 29 (1955), pp. 59-77.

[2] ———, "A general theory of algebraic geometry over Dedekind domains; I," *American Journal of Mathematics*, vol. 78 (1956), pp. 78-116; *ibid.*, vol. 80 (1958), pp. 382-420.

[3] ———, "The theory of multiplicity in general local rings," *Proceedings of the International Symposium on Algebraic Number Theory*, Tokyo-Nikko, 1955 (1956), pp. 191-226.

[4] ———, "A Jacobian criterion of simple points," *Illinois Journal of Mathematics*, vol. 1 (1957), pp. 427-432.

[5] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[6] A. Weil, "Foundation of algebraic geometry," *American Mathematical Society Publications* (1946).

[7] ———, "Fibre-spaces in algebraic geometry," Lecture at the University of Chicago (1952).

[8] O. Zariski, "The concept of a simple point of an algebraic varieties," *Transactions of the American Mathematical Society*, vol. 62 (1947), pp. 1-52.

ON THE TRANSFORMATION THEORY OF ELLIPTIC FUNCTIONS.*[1]

By JUN-ICHI IGUSA.

It has been customary to call the *theory of isogeny of ellipitic curves with "variable moduli"* as transformation theory of elliptic functions. The results of Lagrange and Gauss on arithmetic-geometric means and transformations discovered by Landen and Legendre were the germs of this theory. However, a real initiation was made independently by Abel and Jacobi. This theory was later deepened and completed in an essential way by Kronecker in his well-known series of papers on elliptic functions. Now, in a 1950 congress address, André Weil gave a geometric formulation of the transformation theory and suggested a reconsideration of this "splendid work" from a modern point of view. However, as far as we know, no one has yet worked out his suggestion. This we shall propose to do in this paper. As we know, although the final results are of geometric nature, Kronecker made use of Jacobi elliptic functions and, what is worse, the transformation formulas of Jacobi theta functions in establishing his theory. Now, it seems that any worth-while reconsideration should be along the *strict Kroneckerian programme* and, in particular, it should be of a geometric nature. It is relatively easy to discuss contributions of Abel and Jacobi in a geometric form. However, we encountered with one difficulty in geometrizing Kronecker's theory. In fact, we are thus led to establish a new geometric theory of modular functions, which we shall publish separately. With the aid of this theory, we shall discuss the transformation theory in a *definitive form* which is more precise than Weil's formulation in various respects. We hope that this paper contributes to the clarification of the matter and thus to a future generalization of the theory.

1. Preliminaries. Throughout this paper, we shall assume that the

* Received September 2, 1958.

[1] This work was partially supported by a research grant of the National Science Foundation. The content of this paper was lectured at Johns Hopkins University in the spring term, 1958.

characteristics of fields we consider are different from 2. Moreover, by an elliptic curve we always understand an Abelian variety of dimension 1. We shall denote its neutral element by o. In this section we shall summarize basic results on elliptic curves, which hold actually for any characteristic. Most of them are proved by Hasse in [3]. However, to readers with geometric background, we shall recommend Weil's general treatment [9]. We shall make use of some more results, which we shall mention at suitable places.

Consider the group of divisors of an elliptic curve A. Then the natural epimorphism of this group to the group variety A will be denoted by S. Let $\mathfrak{a}$ be a divisor of A of degree zero. Then $\mathfrak{a}$ belongs to the kernel of S if and only if $\mathfrak{a}$ is a principal divisor, i. e. if and only if there exists a function f on A satisfying $(f)=\mathfrak{a}$. In this way S gives rise to an isomorphism of the divisor class-group of degree zero of A, i. e. the group of divisors of A of degree zero modulo the group of principal divisors of A, to A. We can simply say that A is its own Albanese and Picard variety. On the other hand, if α is a homomorphism of A to another elliptic curve B, then $S\cdot\alpha^{-1}$ is a homomorphism α' of B to A up to a translation in A. The correspondence $\alpha\rightarrow\alpha'$ is an isomorphism of $\mathrm{Hom}(A,B)$ to $\mathrm{Hom}(B,A)$. Moreover $\alpha\alpha'$ is $\deg(\alpha)$ in the sense $\alpha\alpha'(v)=\deg(\alpha)v$ for every point v of B. Here $\deg(\alpha)$ means the mapping degree of α. In a similar sense, we have $\alpha'\alpha=\deg(\alpha)$. If β is a homomorphism of B to another elliptic curve C, we have $(\beta\alpha)'=\alpha'\beta'$ and $(\alpha')'=\alpha$. There is another way to associate a contravariant map to α. In fact, if we consider the vector spaces of invariant differentials of A and B, then α induces a contravariant linear map of these vector spaces. Therefore, if we fix their bases θ_A and θ_B, we get a finite quantity μ by $\theta_B\rightarrow\mu\theta_A$. The quantity μ is called the *multiplicator* of α. The multiplicator of α is zero if and only if α is an inseparable homomorphism. Moreover, in case $A=B$, we can take $\theta_A=\theta_B$. Then the multiplicator of α is uniquely determined by α and the correspondence $\alpha\rightarrow\mu$ is a representation of the ring $\mathrm{Hom}(A,A)$. We note that an invariant differential and an everywhere finite differential are the same.

If n is a natural number, the endomorphism n of A is of degree n^2. This endomorphism is separable if and only if n is not a multiple of the characteristic. In this case, therefore, the kernel is a finite Abelian group of type (n,n). On the other hand, if $\mathfrak{a}$ is a divisor of A of degree zero such that $t=S(\mathfrak{a})$ is a point of order n, we have $S(n^{-1}(\mathfrak{a}))=o$. Hence, there exists a function f on A satisfying $(f)=n^{-1}(\mathfrak{a})$. If s is a point of A of order n and u a general point of A, we have $f(u+s)=e_n(s,t)f(u)$ with some n-th root of unity $e_n(s,t)$. This n-th root of unity depends only on n,

s and t. Moreover, the correspondence $(s,t)\to e_n(s,t)$ is a skew-symmetric pairing of the group of points of A of order n to itself. This fact will play a role immediately in the next section.

There is one more theorem, which is proved by Chow [1]. Let α be, as above, an element of $\mathrm{Hom}(A,B)$. Then α is always defined over a separable extension of a common field of definition of A and B. Actually, as most of the other results, it is proved for general Abelian varieties.

2. Jacobi quartics. Let A be an elliptic curve. Then A carries sixteen points of order four. Pick one, say r, out of twelve primitive fourth division points, i.e. points of exact order four. Then, there exists a function x on A determined up to a constant by $(x)=2^{-1}(0)-2^{-1}(2r)$. Since (x) is invariant under the automorphism $u\to -u$ of A, we have $x(-u)=cx(u)$ with some constant c different from 0. Since the automorphism is of order 2, we get $c^2=1$. However, since $u=0$ is a simple zero of x, as we can see by a specialization argument, it can not be an even function. Therefore x must be an odd function, i.e. we have $x(-u)=-x(u)$. On the other hand, (x) will be transformed into $-(x)$ under the translation $u\to u+r$ of A. Hence, we have $x(u+r)=cx(u)^{-1}$ with some constant c different from 0. *We shall normalize the constant factor of x so that we get $c=1$. Then x is uniquely determined up to its sign and we have $x(u+r)=x(u)^{-1}$.* In particular, x is invariant under the translation $u\to u+2r$ of A. Naturally, this property does not depend on the normalization. Furthermore, x undergoes sign changes by two other translations of A of order 2.

Now, let s be another primitive fourth division point of A such that $2s$ is different from $2r$. We have eight possible s and the mean value ρ of x^2 over these eight points

$$\rho=(\tfrac{1}{8})\sum x^2(s)$$

is uniquely determined by A and $\pm r$. Here we remark this. If σ is one of the $x(s)$, the eight values of $x(s)$ are simply $\pm\sigma$, $\pm\sigma^{-1}$ each with multiplicity 2. Therefore ρ is of the form $\frac{1}{2}(\sigma^2+\sigma^{-2})$ and we have the following relation

$$\prod_s (x(s)-X)=(1-2\rho X^2+X^4)^2.$$

We also make the following remark. If v is a point of A at which x is finite, then, including multiplicity, the zeros of $x-x(v)$ are given modulo $2r$ by v and $-v+2s$. As an application of this fact, we can determine the divisor of the function $1-2\rho x^2+x^4$ on A and we get $2\mathfrak{a}$ with $\mathfrak{a}=\sum(s)-2\cdot 2^{-1}(2r)$.

Since we have $S(\alpha)=0$, we can write $1-2\rho x^2+x^4$ in the form y^2 with some function y on A. Since (y) is invariant under the automorphism $u\to -u$ of A, we see that y is even or odd. However, sinve we have $y^2(0)=1$, it must be an even function, i. e. we have $y(-u)=y(u)$. *We shall normalize* y *uniquely by* $y(0)=1$. The two functions x and y are invariant under the translation $u\to u+2r$ of A and "uniformize" the plane quartic $Y^2=1-2\rho X^2+X^4$, which we call the *Jacobi quartic* of *modulus* ρ.[2] We note that the modulus ρ is different from ± 1 and ∞. It is clear that ρ is finite. If ρ is ± 1, we get $y=1\mp x^2$. However, this is not possible, because y must undergo sign changes by the two translations of A of the form $u\to u+2s$.

Conversely, if ρ is different from ± 1 and ∞, the Jacobi quartic of modulus ρ is absolutely irreducible and the four roots $\pm\sigma$, $\pm\sigma^{-1}$ of $1-2\rho X^2+X^4=0$ are distinct. Moreover, the point at infinity $(0,1,0)$ is the only singularity. Therefore, the quartic is of genus 1 and, if Q is the prime field, we can introduce a normal law of composition over the field $Q(\rho)$ with $(0,1,1)$ as neutral element. *As long as we avoid the double point* $(0,1,0)$, i. e., *as long as we restrict to finite points, we can treat the Jacobi quartic as an elliptic curve.* In fact, the normalization over $Q(\rho)$ transforms the quartic into an elliptic curve and the correspondence is everywhere biregular except at the point at infinity. The *absolute invariant* of this elliptic curve can be calculated, for instance, by transforming it isomorphically into a plane cubic $Y^2=X(1-X)(\lambda-X)$ with $(0,1,0)$ as neutral element. The modulus λ is a cross-ratio of the four roots $\pm\sigma$, $\pm\sigma^{-1}$, hence $\lambda=\frac{1}{2}(1+\rho)$ is one of them. This shows that ρ is also a modular function of level 2 [4]. Moreover, in terms of ρ the absolute invariant can be expressed as follows

$$j=2^6(3+\rho^2)^3(1-\rho^2)^{-2}.$$

Therefore, *if* Z *is the prime integral domain, then* 8ρ *is always integral over* $Z[j]$ *and* 8 *is the smallest natural number having this property.* Moreover, the ρ-space is a Galois covering of the j-space with the symmetric group of permutations of three letters as the Galois group. The covering is ramified at the degenerate case $j=\infty$, the harmonic case $j=12^3$ and the equianharmonic case $j=0$. The corresponding values of ρ are given, respectively, by $\{\pm 1,\infty\}$, $\{0,\pm 3\}$ and $\{\pm(-3)^{\frac{1}{2}}\}$.

On the other hand, if a Jacobi quartic with a non-degenerate modulus ρ,

[2] In the classical case, this quartic was uniformized by Jacobi elliptic functions as $x=\sigma\,\mathrm{sinam}(t,\sigma^2)$ and $y=\mathrm{cosam}(t,\sigma^2)\,\Delta\,\mathrm{am}(t,\sigma^2)$. See Jacobi [6, 7] and Kronecker [8].

i.e. a modulus ρ different from ± 1 and ∞, is given, we can always uniformize it by an elliptic curve A as indicated before. In fact, if we map the normalization of the quartic to an elliptic curve A by a homomorphism α of degree 2, essentially α' gives such a uniformization. We leave to the reader to make it precise. In this way, we can consider either the elliptic curve or the Jacobi quartic as initially given. At any rate, we shall always consider them as a pair. We also make the following rather scattered remarks.

If a_1 and a_2 are points of A of odd orders, then $x(a_1)=x(a_2)$ implies $a_1=a_2$. If u is a variable point of A, then $x(u+s)$ is an even function of u. Also, the differential dx/y is everywhere finite on A, hence it is an invariant differential of A. Proofs are immediate. In the following sections, notations will be always the same. For instance, s means a primitive fourth division point of A such that $2s$ is different from $2r$.

3. Transformation of Jacobi quartics. Let A be an elliptic curve and let α be a homomorphism of an *odd* degree m of A to another elliptic curve A'. Then α induces an isomorphism of the 2-primary parts of the groups of points of finite orders of A and A'. In particular, if r is, as before, a primitive fourth division point of A, then $r'=\alpha r$ is a primitive fourth division point of A'. Let ρ and ρ' be the moduli of Jacobi quartics associated with A and A' with reference to $\pm r$ and $\pm r'$. Also, let x, y and x', y' be the functions which uniformize these quartics. Then α commutes with the translations $u\to u+2r$ and $u'\to u'+2r'$ of A and A', hence α induces a homomorphism of Jacobi quartics of the same degree m as α. Therefore, we can write $x'(\alpha u)$ uniquely in the form $R_0(x)+R_1(x)y$ with $x=x(u)$ and $y=y(u)$. Here $R_0(X)$ and $R_1(X)$ are rational functions of X. If we apply the automorphism $u\to -u$ of A, we see that R_0 and R_1 are both odd. If we apply the translation $u\to u+2s$ of A, we see that R_1 is even. Hence R_1 must be zero and, thus, we simply get $x'(\alpha u)=R(x)$ with an odd rational function $R(X)$ of X. In the same way, we get $y'(\alpha u)=S(x)y$ with some even rational functions $S(X)$ of X. Since we know that the homomorphism $(x,y)\to(x',y')$ is of degree m, the rational function $R(X)$ must be of degree m. In other words, $R(X)$ is a quotient of co-prime polynomials at least one of which is of degree m. Now, if we apply the translation $u\to u+r$ of A, we get $R(X^{-1})=R(X)^{-1}$. Since we also have $R(0)=0$, we can write $R(X)$ in the form $cX^mF(X^{-1})F(X)^{-1}$ with $c^2=1$ and with

$$F(X)=1+\sum_{0\leqq 2i<m-1} c_i X^{m-2i-1}.$$

Here, by changing the sign of x' if necessary, we can make $c=1$. Remember

that x' is determined by r' only up to sign. If we substitute $x' = R(x)$ and $y' = S(x)y$ in $(y')^2 = 1 - 2\rho'(x')^2 + (x')^4$, we see that

$$F(X)^4 S(X)^2 (1 - 2\rho X^2 + X^4)$$

is a polynomial of X. Therefore $G(X) = F(X)^2 S(X)$ must be a polynomial of X and, in fact, a polynomial of X^2. Moreover, $G(X)$ is of degree $2m - 2$ as a polynomial of X and satisfies $G(0) = 1$. With the aid of the polynomials $F(X)$ and $G(X)$, which we call transformation polynomials, the homomorphism $(x, y) \rightarrow (x', y')$ can be expressed as follows

$$x' = x^m F(x^{-1}) F(x)^{-1} \qquad y' = G(x) F(x)^{-2} y.$$

In Kronecker's terminology, *transformation equations* meant always $F(X) = 0$, or rather $X^m F(X^{-1}) = 0$ and mostly in the case of prime transformation degrees. We shall show that the transformation polynomials can be decomposed into linear factors explicitly.

Take a field of definition K of α containing all coefficients of $F(X)$. Let u be a generic point of A over K and put $x' = x'(\alpha u)$. Then x' is transcendental over K, hence $X^m F(X^{-1}) - x' F(X)$ is an irreducible polynomial over $K(x')$. It is easy to determine all distinct roots of this polynomial. At any rate, if a belongs to the kernel of α, certainly $x(u + a)$ is a root. Conversely, if x is an arbitrary root, we can write it in the form $x(v)$ with some point v of A and we get $x'(\alpha v) = x'$. In Section 2, we remarked how to analyse an equation of this type. Thus we get $x(v) = x(u + a)$ with some a in the kernel of α. Also, if a_1 and a_2 are distinct elements of the kernel of α, then $x(a_1)$ and $x(a_2)$, hence also $x(u + a_1)$ and $x(u + a_2)$, are distinct. Therefore, if e is the common multiplicity of the roots and if we denote a typical element of the kernel of α by a, we get

$$X^m F(X^{-1}) - x' F(X) = \prod_a (X - x(u + a))^e.$$

In particular, if we specialize u to 0 over K, we get

$$F(X) = \prod_a (1 - x(a) X)^e.$$

The exponent e is a certain power of the characteristic, and it is called the inseparability degree of α. The number of elements in the kernel of α multiplied by the inseparability degree e of α is the total degree m of α.

Now, in order to obtain a similar decomposition of $G(X)$ into linear factors, we shall explain the notion of a "half system." A half system of a finite Abelian group of an odd order is its subset S which together with

zero and $-S$ sum, without overlapping, to the whole group. We see that a point v of A satisfies $y'(\alpha v)=0$ if and only if v is of the form $s+a$, i.e., if and only if we have $x(v)=x(s+a)$ with some s and a. Here, if we restrict s to representatives modulo $2r$ and a either to 0 or to elements of a half system of the kernel of α, the corresponding $x(s+a)$ are distinct. Since $x(s+u)$ is an even function of u, we do not loose anything by this restriction. Moreover, certainly $x(s+a)$ are different from the roots of $F(X)=0$. Therefore, by using the previous remark, we get

$$G(X)=(1-2\rho X^2+X^4)^{\frac{1}{2}(e-1)}\prod_{\substack{s \bmod 2r\\ a\text{ half system}}}(X-x(s+a))^e.$$

On the other hand, with respect to the invariant differentials dx/y and dx'/y' we can calculate the multiplicator μ of α. In fact, if we observe $y(0)=y'(0)=1$, we get

$$\mu=c_0=\prod_{a\neq 0}x^e(a).$$

In the above discussion, we started from a homomorphism α of an odd degree of elliptic curves A and A' and we studied the induced homomorphism of Jacobi quartics associated with A and A' with reference to $\pm r$ and $\pm\alpha r$. Conversely, suppose that a non-degenerate Jacobi quartic of modulus ρ and a homomorphism $(x,y)\rightarrow(x'',y'')$ of an odd degree m of this quartic to another Jacobi quartic of modulus ρ'' are given. Then, at any rate, we can uniformize the Jacobi quartic of modulus ρ by an elliptics curve A with reference to, say $\pm r$, and we can consider the kernel of the homomorphism $(x,y)\rightarrow(x'',y'')$ as an isomorphic image of a subgroup of A under this uniformization. On the other hand, let e be the inseparability degree of the homomorphism $(x,y)\rightarrow(x'',y'')$. Then the e-th power of the factor group of A by that subgroup, which is obtained by raising the co-ordinates of points to their e-th powers [1], is an elliptic curve. We denote this elliptic curve by A' and the corresponding homomorphism by α. We are thus in the same situation as before; hence we get a homomorphism $(x,y)\rightarrow(x',y')$ of degree m of the Jacobi quartic of modulus ρ to the Jacobi quartic of modulus, say ρ', associated with A' with reference to $\pm\alpha r$. However, since the two homomorphisms $(x,y)\rightarrow(x',y')$ and $(x,y)\rightarrow(x'',y'')$ have the same kernel and the same inseparability degree, the image quartics must be isomorphic. We note that *the homomorphism* $(x,y)\rightarrow(x',y')$ *is uniquely determined by the given homomorphism* $(x,y)\rightarrow(x'',y'')$. In the following, we shall use the word "transformation" for this well-selected homomorphism of Jacobi quartics with variable moduli, i.e. with transcendental moduli over Q. Also,

we indicate the transformation by $(\rho, x, y) \to (\rho', x', y')$. If we polarize A and A' by $\pm r$ and $\pm r'$, the transformation is characterized up to the sign of x' by the commutativity of the following diagram

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & A' \\ \downarrow & & \downarrow \\ (\rho, x, y) & \longrightarrow & (\rho', x', y'). \end{array}$$

This observation facilitates to verify that *a product of transformations is a transformation and that the multiplicator of the product is the product of multiplicators.* Moreover, if a transformation $(\rho, x, y) \to (\rho', x', y')$ is induced by α, then α' induces a transformation of the form $(\rho', x', y') \to (\rho, \pm x, y)$. The sign in front of x will be determined to be $(-4/m) = (-1)^{\frac{1}{2}(m-1)}$ in the next section. At any rate, we call it the *complementary transformation* of the given transformation, a terminology due to Jacobi. If μ is the multiplicator of the original transformation and μ' the one for the complementary transformation, we therefore get $\mu\mu' = (-4/m)m$. Now we shall prove the following theorem.

THEOREM 1. *Let $F(X)$ and $G(X)$ be the transformation polynomials associated with a transformation $(\rho, x, y) \to (\rho', x', y')$. Then the coefficients of $F(X)$ and $G(X)$ are contained in $Q(\rho, \rho')$.*

We first note that the assertion for $G(X)$ follows from the assertion for $F(X)$. In fact, if the coefficients of $F(X)$ are contained in $Q(\rho, \rho')$, the coefficients of $G(X)^2$, hence those of $G(X)$, must also be contained in the same field. We know by Chow's theorem that the coefficients of $F(X)$ are separable over $Q(\rho, \rho')$. Therefore, we have only to show that the kernel of the transformation is normally algebraic over $Q(\rho, \rho')$. If the kernel is not normally algebraic over $Q(\rho, \rho')$, as we can see, such a bad situation happens already by a transformation with cyclic kernel of the transformation degree not divisible by the characteristic. Therefore, we can assume that we have such a case from the beginning. However, this is not possible, because factor groups by distinct cyclic subgroups of the same order have even distinct absolute invariants [4]. This completes the proof.

Actually, in proving Theorem 1 we could have used the Galois theory of division points [4]. The proof would, then, become less formal. However, the above proof is of an elementary nature.

4. Multiplication of Jacobi quartics. If n is an odd natural number, the endomorphism n of A is of degree $m = n^2$ and maps r to $r' = (-4/n)r$. Therefore x' differs from x at most by sign and we have $\rho' = \rho$. In this case, the transformation is called a *multiplication* and we shall denote the corresponding polynomials by $F_n(X)$ and $G_n(X)$. We already encountered with a multiplication implicitly in the proof of Theorem 1. At any rate, $F_n(X)$ and $G_n(X)$ are polynomials of X with coefficients in $Q(\rho)$. Moreover, these polynomials are *universal* in the sense they are compatible with specializations. Here, as we agreed in Section 1, the reduction modulo 2 should be excluded. The following theorem is fairly deep and the crucial point of the proof is along Kronecker's idea.

THEOREM 2. *The coefficients of multiplication polynomials $F_n(X)$ and $G_n(X)$ are contained in $Z[8\rho]$.*

We can assume, because of the universality and of the nature of the theorem, that the characteristic of Q is zero. We shall first show that the assertion for $G_n(X)$ follows from the assertion for $F_n(X)$. In fact, the relation $dx(nu)/y(nu) = ndx/y$ shows that the coefficients of $nG_n(X)$ are contained in $Z[8\rho]$. On the other hand, $G_n(X)^2$ is a polynomial of X with coefficients in $Z[2\rho]$, hence in $Z[\rho]$. Since $G_n(X)$ satisfies $G_n(0) = 1$, by the so-called Gauss lemma, the coefficients of $G_n(X)$ itself must be contained in $Z[\rho]$. Therefore, the coefficients of $G_n(X)$ are contained in $Z[8\rho]$. In order to prove the assertion for $F_n(X)$, we must obtain the addition theorem for x. Incidentally, the subsequent discussion holds without the restriction on the characteristic. Let v and w be independent generic points of A over a common field of definition K of x and y. Put $v + w = u$ and take the field $K(x(u), y(u))$ as our domain of rationality. Then $x_1 = x(v)$ and $x_2 = x(w)$ are related by an irreducible symmetric equation which is quadratic in x_1 and in x_2 individually over this domain of rationality. If we make the translations $v \to v + 2s$ and $w \to w + 2s$ of A simultaneously, then x_1 and x_2 change their signs, hence the equation contains neither $x_1x_2(x_1 + x_2)$ nor $x_1 + x_2$. Furthermore, since we can make the translations $v \to v + r$ and $w \to w + r$ of A over the domain of rationality, the coefficient of $x_1^2x_2^2$ is equal to the constant term. Thus the equation takes the following form

$$\gamma_0(x_1^2x_2^2 + 1) + 2\gamma_1x_1x_2 + \gamma_2(x_1^2 + x_2^2) = 0.$$

Here, if we specialize v to u and w to 0 over the domain of rationality, we get $\gamma_0 + \gamma_2x^2(u) = 0$. Moreover, in order to solve the above equation in x_2, we must extract a quadratic radical from $\gamma_1^2x_1^2 - (\gamma_0 + \gamma_2x_1^2)(\gamma_0x_1^2 + \gamma_2)$.

Since x_2 must be contained in $K(x_1, y_1)$, therefore, this polynomial of x_1 must be a multiple of $1-2\rho x_1^2+x_1^4$. In this way, we see that the expression for x_2 takes the following form

$$x(u-v)=(x(u)y(v)-x(v)y(u))(1-x^2(u)x^2(v))^{-1}.$$

Once we have this formula, by specializing v to $-u$ over K we get $x(2u) = 2xy(1-x^4)^{-1}$ with $x=x(u)$ and $y=y(u)$. Now, assume that the theorem is true up to n and specialize u to nu and v to $-2u$ over K. Then, if we observe $dx(2u)/y(2u)=2dx/y$ and $y(nu)=G_n(x)F_n(x)^{-2}y$, we see that $x((n+2)u)$ is of the form $N(x)D(x)^{-1}$ with

$$D(X)=(1-X^4)^2F_n(X)^2-4X^2(1-2\rho X^2+X^4)X^mF_n(X^{-1}).$$

The numerator $N(X)$ is, at any rate, a polynomial of X with coefficients in $Z[\rho]$. We observe that the coefficients of $D(X)$ are contained in $Z[8\rho]$ and $D(X)$ satisfies $D(0)=1$. Since $F_{n+2}(X)$ also satisfies $F_{n+2}(0)=1$ and divides $D(X)$ in the polynomial ring $Q(\rho)[X]$, by the Gauss lemma the division must take place within the coefficient domain $Z[8\rho]$. This completes the proof.

COROLLARY 1. *The coefficients of transformation polynomials $F(X)$ and $G(X)$ are integral over $Z[8\rho]$. Moreover, the roots of $G(X)=0$ are units over $Z[8\rho]$.*

The main assertion follows from the fact that $x(a)$ and $x(s+a)$ are integral over $Z[8\rho]$ by Theorem 2. The additional statement is a consequence of the fact that the highest coefficient of $G(X)$ as well as the constant term are 1. In connection with this, we shall show that the highest coefficient c_0 of the multiplication polynomial $F_n(X)$ is $(-4/n)n$. At any rate c_0 is the product of $x^2(a)$ extended over a half system. We are assuming, because of the universality, that the characteristic is zero. If we specialize ρ to 1, by a specialization argument, we see that n^2-n of the $x^2(a)$ specialize to 1 and c_0 will become a product of $x'^2(a')$, say, extended over a half system. Since the specialized addition theorem is of the form

$$x'(u'+v')=(x'(u')+x'(v'))(1+x'(u')x'(v'))^{-1},$$

we see that the product in question is $(-4/n)n$, as asserted. We also add the following corollary.

COROLLARY 2. *Let $(\rho, x, y)\rightarrow(\rho', x', y')$ be a transformation and put $\sigma=x(s)$ and $\sigma'=x'(\alpha s)$. Then $\sigma'\sigma^{-1}$ is a unit over $Z[8\rho]$, hence $2\rho'$ is integral over $Z[2\rho]$.*

In general, as we see from the addition theorem for x, the product $x(u+v)x(u-v)$ can be written in the form

$$(x^2(u)-x^2(v))(1-x^2(u)x^2(v))^{-1}.$$

Therefore, we can write σ' as follows

$$\begin{aligned}\sigma' &= (\prod_{a}(x(s)-x(a))(1-x(a)x(s))^{-1})^{e}\\ &= x^{e}(s)(\prod_{a\,\text{half system}}(x^2(s)-x^2(a))(1-x^2(a)x^2(s))^{-1})^{e}\\ &= \sigma^{e}\prod_{a\,\text{half system}} x^{2e}(s+a).\end{aligned}$$

On the other hand, σ is a unit over $Z[2\rho]$ as a root of $1-2\rho X^2+X^4=0$ and, of course, we have $e=1$ in the case of characteristic zero. The corollary follows immediately from these facts and from the above expression for σ'.

5. A digression. In reviewing known results in Section 1, we did not mention properties of *Hasse invariant.* Actually, Kronecker seemed to know the full meaning of this invariant, which we shall discuss by a slightly different purely algebraic method. In general we can expand $(1-2\rho x^2+x^4)^{-\frac{1}{2}}$ in a formal power-series of x as follows

$$(1-2\rho x^2+x^4)^{-\frac{1}{2}}=\sum_{i=0}^{\infty}P_i(\rho)x^{2i}.$$

The coefficients $P_0(\rho)=1, P_1(\rho),\cdots$ are the so-called *Legendre polynomials.* If the characteristic is zero, we can integrate the differential equation $dt=dx/y$ by a formal power-series $t=x+\cdots$. This power-series can be inverted and we get $x=t+\cdots$. Call it $f(t)$. Then we can expand $f(nt)$ in a formal power-series of x. Also, we can expand $x(nu)$ in a formal power-series of $x=x(u)$. The addition theorem of invariant differentials guarantees that these two expansions are the same. If n is a prime number p, from this we can derive congruence properties of the coefficients of the multiplication polynomial $F_p(X)$. For instance, it is quite easy to get the following congruence relations

$$c_i\equiv(-4/n)(p/(2i+1))P_i(\rho) \bmod p^2$$

for $i=0,1,\cdots,\frac{1}{2}(p-1)$. In particular, if we take the last congruence relation modulo p, we get

$$\prod_{\substack{pa=0\\ a\neq 0}} x^{p}(a)=(-4/n)P(\rho)$$

with $P(\rho)=P_{\frac{1}{2}(p-1)}(\rho)$. Therefore, we have $P(\rho)=0$ if and only if A has

no point of order p except o. On the other hand, since $P(\rho)$ is the $\frac{1}{2}(p-1)$-th Legendre polynomial, it satisfies the Legendre differential equation, which in the case of characteristic p, takes the following form

$$(1-\rho^2)d^2P/d\rho^2-2\rho dP/d\rho-(\tfrac{1}{4})P=0.$$

Here $P(\pm 1)$ is different from zero; hence *from the differential equation it follows that the* $\frac{1}{2}(p-1)$ *roots of* $P(\rho)=0$ *are simple.* The Galois group of the ρ-space over the j-space operates on this set of $\frac{1}{2}(p-1)$ roots and we can count the number of orbits quite easily using results in Section 2. This number is precisely the number of non-isomorphic elliptic curves in characteristic p having no point of order p except neutral element. We have already discussed this topic, including the meaning of the coefficient $\frac{1}{4}$, in a separate paper [5]. At any rate, this was how we got the well-known Gauss differential equation for an explicit form of Hasse invariant calculated by Deuring [2] using Hasse's theory.

If we also take into account the fact that $P(\rho)=0$ implies $F_p(X)=1$, we see that the non-vanishing coefficients of $F_p(X)$ in characteristic p are divisible by $P(\rho)$. In other words, we can write $F_p(X)$ in the form

$$F_p(X)=1+\sum_{0<2i<p-1}P(\rho)\gamma_i(\rho)X^{(p-2i-1)p}+(-4/p)P(\rho)X^{(p-1)p}$$

with certain polynomials $\gamma_1(\rho),\gamma_2(\rho),\cdots$ of ρ with coefficients in Z. There is a formal analogy between this relation and the Kronecker conguence relation which we shall discuss in the last section.

6. **Absolute irreducibility of certain equations.** We come to the section where our geometric theory of modular functions plays a role. As before, let n be an odd natural number and assume that the modulus ρ is transcendental over Q. We assume, in addition, that n is not divisible by the characteristic. If a is a point of A of order n, then $x(a)$ is integral over $Z[8\rho]$. Moreover, if we put

$$\Phi_n(X)=\prod_{a\text{ primitive}}(X-x(a)),$$

then $\Phi_n(X)$ is a polynomial of X^2 with coefficients in $Q(\rho)$. The coefficients are, therefore, contained in $Z[8\rho]$, hence we can write $\Phi_n(X)$ in the form $\Phi_n(X^2,8\rho)$ with a polynomial $\Phi_n(X,Y)$ of X and Y with coefficients in Z. We call $\Phi_n(X,Y)=0$ the n-th *division equation.* In the simplest case $n=3$, the division equation reads as $X^4-6X^2+XY-3=0$. In general, if we denote the Euler function by $\phi(n)$ and the number of cyclic subgroups of

order n in the group of points of A of order n by $\psi(n)$, we can easily calculate the degree and the constant term of $\Phi_n(X)$ and we get

$$\deg \Phi_n(X) = \phi(n)\psi(n) = n^2 \prod_{p \mid n} (1 - p^{-2})$$

$$\Phi_n(0) = \begin{cases} (-4/n)p & n = p^e \\ (-4/n) & \text{otherwise.} \end{cases}$$

Here p means a prime number. We can use, for instance, the so-called Möbius inversion formula to make the calculation. At any rate, *in case n contains two distinct prime factors, the roots of $\Phi_n(X) = 0$ are units over* $Z[8\rho]$. Now, we shall prove the following theorem.

THEOREM 3. *The division equation $\Phi_n(X, Y) = 0$ is absolutely irreducible.*

Let λ' be transcendental over Q and consider the plane cubic $Y^2 = X(1-X)(\lambda'-X)$ with $(0, 1, 0)$ as neutral element. We take this elliptic curve as A. Let Ω be the group of points of A of order n. Also, let k be the algebraic closure of Q and adjoin the points of A of order four to $k(\lambda')$. Then we get an extension K of $k(\lambda')$. The Galois group of $K(\Omega)$ over K operates on Ω and, with respect to a base of Ω, we get a representation by two-by-two integer matrices of determinant 1 modulo n. The point is that we get all such matrices in this way [4, Theorem 1]. On the other hand, x^2 is defined over K and ρ is contained in K. Moreover ρ is certainly transcendental over Q. Since the only conjugates of a over $K(x^2(a))$ are a and $-a$, we see that the Galois group of $K(x^2(a))_{na=0}$ over K is what we denoted by $LF(2, n)$ in [4], which is the whole group of two-by-two integer matrices of determinant 1 modulo n divided by plus and minus of the unit matrix. As a consequence, the Galois group operates transitively on the roots of $\Phi_n(X, 8\rho) = 0$. Therefore $\Phi_n(X, 8\rho)$ is irreducible over K. This is already much stronger than Theorem 3.

There are two significant equations which are "derived" successively from the division equation. Consider a transformation $(\rho, x, y) \to (\rho', x', y')$ of degree n with cyclic kernel. Since we have $\psi(n)$ possibilities for the kernel, we have the same number of distinct moduli ρ'. Since $2\rho'$ is integral over $Z[2\rho]$, we get a polynomial $\Psi_n(X, Y)$ of X and Y with coefficients in Z of degree $\psi(n)$ in X satisfying

$$\Psi_n(X, 2\rho) = \prod_{\rho'} (X - 2\rho').$$

We call $\Psi_n(X, Y) = 0$ the n-th *modular equation*. The existence of the

complementary transformation and the irreducibility of $\Psi_n(X, Y)$ which we shall prove presently show that $\Psi_n(X, Y)$ is symmetric in X and Y. For example, the third modular equation reads as follows

$$(X^3 - Y)(X - Y^3) - 3[5X^3Y^3 + 2.31X^2Y^2 + 5.17XY \\ - 2^25XY(X^2 + Y^2) - 2^8(X^2 + Y^2) + 2^{10}] = 0.$$

This suggests that modular equations have less complicated numerical coefficients than "invariant transformation equations."

On the other hand, if μ is the multiplicator of the transformation $(\rho, x, y) \to (\rho', x', y')$, since μ is integral over $Z[8\rho]$, we get a polynomial $M_n(X, Y)$ of X and Y with coefficients in Z of degree $\psi(n)$ in X satisfying

$$M_n(X, 8\rho) = \prod_{\rho'} (X - \mu).$$

We do not know apriori that the $\psi(n)$ roots of $M_n(X, 8\rho) = 0$ are distinct. At any rate, we call $M_n(X, Y) = 0$ the n-th *multiplicator equation*. The third multiplicator equation reads as $X^4 - 6X^2 - XY - 3 = 0$. In general, the constant term $M_n(0, 8\rho)$, which will turn out to be the norm of μ taken from $Q(\rho, \mu)$ to $Q(\rho)$, can be calculated without difficulty and we get

$$M_n(0, Y) = \prod_{p \mid n} (-4/p)^{\frac{1}{2}e(e+1)} p^{E_p}$$

with

$$E_p = ((p^e - 1)/(p - 1))\psi(n/p^e).$$

Here p^e is the contribution of p to n. In particular, for $n = p$ the constant term is simply $(-4/p)p$. We note that $\Phi_n(X, Y)$, $\Psi_n(X, Y)$ and $M_n(X, Y)$ are universal like $F_n(X)$ and $G_n(X)$. We shall now prove the following theorem.

THEOREM 4. *The modular equation $\Psi_n(X, Y) = 0$ and the multiplicator equation $M_n(X, Y) = 0$ are both absolutely irreducible.*

We know that we have $\psi(n)$ distinct transformed moduli ρ'. Moreover, if we use the same notation as in the proof of Theorem 3, we see that the Galois group of $K(x^2(a))_{na=0}$ over K operates transitively on these moduli. This proves the absolute irreducibility of the modular equation. The same proof can be applied to the multiplicator equation once we are sure that the $\psi(n)$ multiplicators are distinct. Suppose that two distinct transformations $(\rho, x, y) \to (\rho', x', y')$ and $(\rho, x, y) \to (\rho'', x'', y'')$ have the same multiplicator. Then the complementary transformation of the first multiplied by the second is a transformation of the form $(\rho', x', y') \to (\rho'', \pm x'', y'')$ with $\pm n$ as multi-

plicator. If the kernel of this transformation is not cyclic, a multiplication can be factored. In this way, by changing the notation, we are led to the situation where the $\psi(n)$ transformations $(\rho, x, y) \to (\rho', x', y')$ have the same rational multiplicator m, i.e.

$$m = \prod_{i=1,\cdots,n-1} x(ia) = (-4/n) \prod_{i=1,3,\cdots,n-2} x^2(ia)$$

for some element m of Z. However, there certainly exists an extension of the specialization $\rho \to \infty$ over Q in which $x(a)$; hence $x(ia)$ for $i = 1, 3, \cdots, n-2$, are specialized to ∞. This is a contradiction. Therefore, the multiplicators are distinct and the multiplicator equation is absolutely irreducible.

COROLLARY. *If μ is the multiplicator of the transformation $(\rho, x, y) \to (\rho', x', y')$, we have $Q(\rho, \rho') = Q(\rho, \mu)$.*

7. **Kronecker's congruence relation.** Assume now that the degree of the transformation $(\rho, x, y) \to (\rho', x', y')$ is an odd prime number p different from the characteristic of Q. Then we can prove the following theorem.

THEOREM 5. *The transformation polynomial $F(X)$ for the transformation of degree p can be written in the form*

$$F(X) = 1 + \sum_{0<2i<p-1} \mu\gamma_i X^{p-2i-1} + \mu X^{p-1}.$$

Here $\gamma_1, \gamma_2, \cdots$ are integers of $Q(\rho, \mu)$ with reference to $Z[8\rho]$. Moreover, the norm of μ taken from $Q(\rho, \mu)$ to $Q(\rho)$ is $(-4/p)p$.

We proved the additional part in a more general form in the previous section. As for the main assertion, it is trivial in the case of positive characteristic, because μ is then a unit of $Q(\rho, \mu)$ with reference to $Z[8\rho]$. Therefore, we shall assume that the characteristic is zero. Then, the norm of μ taken from $Q(\rho, \mu)$ to $Q(\rho)$ generates a prime ideal in $Z[8\rho]$. Therefore, from the ideal theory of integrally closed Noetherian domains [10], we can conclude that μ generates a prime ideal in the principal order of $Q(\rho, \mu)$ with reference to $Z[8\rho]$. Moreover, we know that the coefficients $c_1, c_2, \cdots$ of $F(X)$ are elements of the same principal order. Since there exists a reduction modulo p in which $x(ia)$ for $i = 1, \cdots, p-1$, and μ are mapped to zero, while ρ remains to be a variable modulus, we see that $c_1, c_2, \cdots$ are multiples of μ. In other words, if we write $c_1, c_2, \cdots$ in the form $\mu\gamma_1, \mu\gamma_2, \cdots$, then $\gamma_1, \gamma_2, \cdots$ must belong to the principal order of which we are talking. This completes the proof.

In a slightly ambiguous way, the main part of Theorem 5 can be expressed

simply by the following congruence relation

$$x'(\alpha u) \equiv x^p(u) \mod \mu.$$

This is the *Kronecker congruence relation.* As he himself confirmed, this congruence relation has a fundamental meaning for the entire transformation theory of elliptic functions as well as its arithmetic applications.

We add a remark about the connection between Theorem 5 and a formula we obtained in Section 5. Let μ' be the multiplicator of the compelementary transformation $(\rho', x', y') \to (\rho, (-4/p)x, y)$ of $(\rho, x, y) \to (\rho', x', y')$. Then, as we know more generally, we have $\mu\mu' = (-4/p)p$. In particular, μ and μ' are both elements of $Q(\rho, \rho')$. Now, we know that the relation between ρ and ρ' is symmetric. Since $2\rho'$ is integral over $Z[2\rho]$, and conversely, we see that the principal order of $Q(\rho, \rho')$ with reference to $Z[2\rho]$ is also the principal order of $Q(\rho, \rho')$ with reference to $Z[2\rho']$. Apparently, this principal order contains the principal orders of $Q(\rho, \rho')$ with reference to $Z[8\rho]$ and $Z[8\rho']$. Therefore, by the same reason as in the proof of Theorem 5, we see that μ and μ' generate prime ideals in that principal order. These prime ideals are distinct, because they even have different norms taken from $Q(\rho, \rho')$ to $Q(\rho)$, say. Now, if $F_p(X)$ is the multiplication polynomial and if we reduce $F_p(X)$ modulo μ', we get

$$F_p(X) \equiv 1 + \sum_{0<2i<p-1} \mu^p \gamma_i^p X^{(p-2i-1)p} + \mu^p X^{(p-1)p} \mod \mu'.$$

If we compare this relation with the formula in Section 5, we get, for instance, the following relation

$$\mu^p \equiv (-4/p) P(\rho) \mod \mu'.$$

Finally, we add some remarks concerning the first non-trivial case $p=5$ for Theorem 5. We know that Kronecker already mentioned this case in [8]. However, our precise theory contradicts some of his calculations. Thus, in order to avoid misunderstandings, we must point out his mistakes. First, the fifth division equation should read as follows

$$\begin{aligned} &X^{12} - 50X^{10} + 35YX^9 - (10Y^2 + 125)X^8 + (Y^3 + 92Y)X^7 \\ &\quad - (15Y^2 + 300)X^6 + 90YX^5 - 105X^4 - 20YX^3 \\ &\quad + (Y^2 + 62)X^2 - 5YX + 5 = 0. \end{aligned}$$

Thus, by reduction modulo 5 we get $X^2(X^{10} + (Y^2+2)YX^5 + (Y^2+2)) = 0$. In Kronecker [8, p. 454], the coefficient of X^7 reads, in our notation, as

$Y^3 + 368$, which seems to be a misprint. Second, the equation for $\gamma = \gamma_1$ should read as follows

$$\gamma^6 + 8\rho \cdot \gamma^5 + 20\gamma^4 - 80\gamma^2 - 16 \cdot 8\rho \cdot \gamma - (8\rho)^2 = 0.$$

Thus γ is, indeed, integral over $Z[8\rho]$. In Kronecker [8, p. 452], intermediate terms seem to be miscalculated.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] W. L. Chow, "Abelian varieties over function fields," *Transactions of the American Mathematical Society*, vol. 78 (1955), pp. 253-275.

[2] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität*, vol. 14 (1941), pp. 197-272.

[3] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper," I, *Journal für die reine und angewandte Mathematik*, vol. 175 (1936), pp. 55-62; II, *ibid.*, pp. 69-88; III, *ibid.*, pp. 193-208.

[4] J. Igusa, "Fibre systems of Jacobian varieties," III, to appear in the *American Journal of Mathematics*.

[5] ———, "Class number of a definite quaternion with prime discriminant," *Proceedings of the National Academy of Sciences*, vol. 44 (1958), pp. 312-314.

[6] C. G. J. Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, 1829, *Collected Works*, vol. 1 (1881), pp. 49-239.

[7] ———, "Suite des notices sur les fonctions elliptiques," 1829, *Collected Works*, vol. 1 (1881), pp. 266-275.

[8] L. Kronecker, "Zur Theorie der elliptischen Functionen," 1883-89, *Collected Works*, vol. 4 (1929), pp. 345-497.

[9] A. Weil, *Variétés Abéliennes et courbes algébriques*, Paris (1948).

[10] O. Zariski and P. Samuel, *Commutative algebra*, New York (1958).

FIBRE SYSTEMS OF JACOBIAN VARIETIES.*[1]

(III. Fibre Systems of Elliptic Curves.)

By JUN-ICHI IGUSA.

To Zariski on his 60th birthday

1. Introduction. This is the third paper on fibre systems of Jacobian varieties. We shall apply some of our previous results [7, 9] to the simplest case of fibre systems of elliptic curves. In this way we get a *geometric theory of elliptic modular functions* with arbitrary level in the sense of Klein [11] for any characteristic which does not divide the level. Here we would like to state that no algebraic theory of modular functions has been available even in the case of characteristic zero. In fact, the known theory depends heavily either on Riemann's existence theorem or on the use of Eisenstein series.

The theory of modular functions in positive characteristic is useful in discussing arithmetic properties of modular functions in characteristic zero. For instance, we can solve the so-called "generalized Ramanujan conjecture" in a *definitive form* for dimension -2. We are following here the general method, orginated by Galois, for constructing a theory in positive characteristic and applying this theory to problems in characteristic zero. In addition to the above mentioned application, which we shall discuss in a separate paper, our theory also contributes to the "three points ramification problem." In fact, we can now construct canonically a Galois covering of a straight line which is ramified at either three or in some cases two points and having $LF(2,n)$ as Galois group, provided n is not a multiple of the characteristic. The reader will find more precise statements in Theorem 4 and Theorem 6. We note that, at least in the case of characteristic zero, these theorems characterize the field of modular functions uniquely. We also note that Gierster's theorem which shows that $LF(2,p)$ contains the tetrahedral group for any odd prime number p is automatically contained in Theorem 6.

* Received September 2, 1958.

[1] This work was partially supported by a research grant of the National Science Foundation. The content of this paper was discussed on March 18, 1958 in a seminar at Harvard University conducted by Professor Zariski.

2. Absolute invariant. Let A be an elliptic curve, i. e. an Abelian variety of dimension 1. We are going to associate a finite quantity $f(A)$ to A, which is contained in the universal domain of A, so that f satisfies the following conditions:

(1) *We have* $f(A)=f(B)$ *if and only if* A *and* B *are isomorphic;*

(2) *If* A' *is a specialization of* A, *then* $f(A')$ *is the unique specialization of* $f(A)$ *over this specialization.*

Here we are assuming, of course, that B and A' are elliptic curves. Moreover, unequal-characteristic specialization [cf. 14] is also included in the second condition. In the following we shall construct f by examining *normal forms* of elliptic curves due to *Legendre* and *Hesse*. As the reader will see, the construction is not quite arbitrary and it turns out that f is unique up to the transformation $f\rightarrow \pm f+\text{integer}$.[2] Observe beforehand that $f(A)$ must be contained in every field of definition of the "underlying" curve of A.

To begin with, we shall recall a *theorem of Hasse*: Let n be a natural number and let u be a typical point of an elliptic curve A. Then the mapping $u\rightarrow n\cdot u$, which is an endomorphism of A, is of degree n^2. The mapping in question is separable if and only if n is not a multiple of the characteristic. In this case, therefore, the kernel is a finite Abelian group of type (n,n). However, in case n is a multiple of the characteristic, the kernel has a different structure depending on the behavior of the Kronecker-Hasse invariant of A [5, 13]. At any rate, let 0 be the neutral element of A. Then the complete linear system on A determined by $3\cdot 0$ gives rise to an isomorphism of A to a plane cubic such that the image of 0 is a flection point. Therefore we can assume from the beginning that A is a plane cubic with a flection point as its neutral element. Then three points u, v, w of A satisfy $u+v+w=0$ if and only if they are collinear. Therefore, as we can see, if B is isomorphic to A, the isomorphism is induced by a linear collineation.

In case the characteristic is different from 2 and only in such case A contains three points of order 2 besides 0 by the above mentioned theorem of Hasse. Moreover these three points are collinear. Therefore we can take the straight line passing through these points as X-axis. Also we take the flection tangent at 0 as Z-axis, i. e. the line at infinity, and a line joining 0 to one of the three points of order 2 as Y-axis. This is possible, because these three straight lines can not go through one same point. Furthermore we can assume

[2] The possibility of unique characterization was suggested by Professor Weil when the author met him at Princeton in January, 1958.

that one of the two remaining points of order 2 has co-ordinates $(1,0,1)$. Here we agree once for all to write co-ordinates in the order X, Y, Z. If the third point has co-ordinates $(\lambda,0,1)$, the equation of the cubic reads as $\alpha\cdot Y^2Z = X(X-Z)(X-\lambda Z)$ with $\alpha\neq 0$. If we replace $\alpha^{\frac{1}{2}}\cdot Y$ by Y, we can write the equation as follows

$$Y^2Z = X(X-Z)(X-\lambda Z).$$

Here the *modulus* λ is different from 0, 1, ∞ and conversely, if that is so, the above equation defines a non-singular cubic. This geometric consideration shows that we have twelve choices for the normalized co-ordinate systems and, accordingly, we get the following six values for the moduli

$$\begin{array}{lll} \lambda & 1-\lambda & (\lambda-1)\lambda^{-1} \\ \lambda^{-1} & (1-\lambda)^{-1} & \lambda(\lambda-1)^{-1}. \end{array}$$

More precisely, the corresponding six cubics, with $(0,1,0)$ as o, are isomorphic and the twelve isomorphisms can be given inhomogeneously by the corresponding generic points as follows

$$\begin{array}{ll} (x,\pm y) & (1-x,\pm(-1)^{\frac{1}{2}}\cdot y) \\ (x\lambda^{-1},\pm\lambda^{-\frac{3}{2}}\cdot y) & ((1-x)(1-\lambda)^{-1},\pm(\lambda-1)^{-\frac{3}{2}}\cdot y) \end{array}$$
$$((\lambda-x)\lambda^{-1},\pm(-\lambda)^{-\frac{3}{2}}\cdot y)$$
$$((\lambda-x)(\lambda-1)^{-1},\pm(1-\lambda)^{-\frac{3}{2}}\cdot y).$$

We can consider those six values of moduli as defining a transformation group operating on a projective straight line. The orbits consist of six points in general except for the *degenerate case* $\{0,1,\infty\}$, the *harmonic case* $\{-1,\frac{1}{2},2\}$ and the *equianharmonic case* $\{-\rho,-\rho'\}$ with respective multiplicities 2, 2 and 3. Here ρ and ρ' are primitive third roots of unity. We note that our group is operating on $\{0,1,\infty\}$ as symmetric group. According to Lüroth's theorem, we can identify these orbits to single points of a projective straight line. Since we have three freedoms at our disposal, we can do this in such a way that the first and the third exceptional orbits are mapped respectively to ∞ and 0. Then up to a constant factor the identification mapping has the following form

$$j = 2^8(\lambda^2-\lambda+1)^3 : \lambda^2(\lambda-1)^2.$$

This j is called the *absolute invariant* of A. We note that the second exceptional orbit is mapped to 12^3. In case the characteristic is 3 the situation is slightly different. We have only two exceptional orbits $\{0,1,\infty\}$ and $\{-1\}$

with respective multiplicities 2 and 6. However, apparently the same j as above works also in this case. We also note that the Lüroth theorem was used only to motivate the reasoning.

In the case of characteristic 2 or, more generally, if the characteristic is different from 3 and only in such case A contains nine flection points, i.e. points of order 3 by Hasse's theorem. As before, let ρ and ρ' be the primitive third roots of unity. Then, as we can see, it is possible to choose a co-ordinate system so that the nine flection points have the co-ordinates $(0,-1,1)$, $(0,-\rho,1)$, $(0,-\rho',1)$; $(1,0,-1)$, $(\rho,0,-\rho')$, $(\rho',0,-\rho)$; $(-1,1,0)$, $(-1,\rho',0)$, $(-1,\rho,0)$. Consequently the equation of the cubic reads as

$$X^3+Y^3+Z^3=3\mu XYZ.$$

Here the *modulus* μ is different from 1, ρ, ρ', ∞ and conversely, if that is so, the above equation defines a non-singular cubic. If we agree to take $(-1,1,0)$ as o, we have four choices for Z-axis. Then the other axes are determined up to a permutation, which reflects the automorphism $u\to -u$ of A. Since Z can be multiplied by an arbitrary third root of unity, we have twenty-four choices for the normalized co-ordinate systems and, accordingly, we get the following twelve values for the moduli

$$\zeta\mu \qquad \zeta(\mu+2\zeta')(\mu-\zeta')^{-1}.$$

The twenty-four isomorphisms themselves can be given inhomogeneously, up to permutations of co-ordinates, by the corresponding generic points as follows

$$(\zeta x,\zeta y)$$
$$(\zeta(\rho x+\rho' y+\zeta')(x+y+\zeta')^{-1},\ \zeta(\rho' x+\rho y+\zeta')(x+y+\zeta')^{-1}).$$

Here ζ and ζ' are the third roots of unity. We can consider those twelve values of moduli as defining a transformation group operating on a projective straight line. The orbits consist of twelve points in general except for the *degenerate case* $\{1,\rho,\rho',\infty\}$, the *harmonic case* $\{1\pm 3^{\frac{1}{2}}, (1\pm 3^{\frac{1}{2}})\rho, (1\pm 3^{\frac{1}{2}})\rho'\}$ and the *equianharmonic case* $\{0,-2,-2\rho,-2\rho'\}$ with respective multiplicities 3, 2 and 3. We note that our group is operating on $\{1,\rho,\rho',\infty\}$ as alternating group. Again we can identify these orbits to single points of a projective straight line so that the first and the third exceptional orbits are mapped respectively to ∞ and 0. Then up to a constant factor the identification mapping has the following form

$$j=3^3\mu^3(\mu^3+2^3)^3:\ (\mu^3-1)^3.$$

This j is called the *absolute invariant* of A. We note that the second excep-

tional orbit is mapped to 12^3. In case the characteristic is 2 the situation is slightly different. We have only two exceptional orbits $\{1, \rho, \rho', \infty\}$ and $\{0\}$ with respective multiplicities 3 and 12. However, apparently the same j as above works also in this case. We note that in case the characteristic is different from 2 and 3 both normalizations are possible. In this way we get an algebraic correspondence between λ-space and μ-space. If λ and μ correspond to each other, they give rise to one and the same j. The correspondence $A \to j(A)$, therefore, satisfies the condition (1) stated in the beginning. Moreover, it is a simple exercise to show that j also satisfies the condition (2). As for the general expression of a correspondence f in the form $f = \pm j +$ integer, it is obvious from the construction of j.

There is another normal form, due to Deuring [3], which is valid provided A contains at least one flection point besides o. This is certainly the case if the characteristic is different from 3, and we shall assume this to be satisfied. Take the line joining these two flection points as Y-axis and the flection tangents as two other axes so that o is represented by $(0, 1, 0)$. If we normalize the co-ordinate system so that the third flection point on the Y-axis has co-ordinates $(0, 1, 1)$, the equation of the cubic reads as $Y^2Z - YZ^2 = \beta \cdot X^3 + 3\nu XYZ$ with $\beta \neq 0$. If we replace $\beta^{\frac{1}{3}} \cdot X$ by X, we can write the equation as follows

$$Y^2Z - YZ^2 = X^3 + 3\nu XYZ.$$

Here the *modulus* ν is different from 1, ρ, ρ', ∞ and conversely, if that is so, the above equation defines a non-singular cubic. Furthermore, for instance, if we make the co-ordinate transformation

$$X : Y : Z \to \rho\mu\nu^{-1}Z : X + \rho' Y + \rho\mu Z : -\rho(X + Y + \mu Z),$$

then $Y^2Z - YZ^2 = X^3 + 3\nu XYZ$ is transformed into $X^3 + Y^3 + Z^3 = 3\mu XYZ$. Here μ and ν are related by $(\mu^3 - 1)(\nu^3 - 1) = 1$. Therefore the absolute invariant can be expressed in terms of ν as follows

$$j = 3^3\nu^3(3^3\nu^3 - 2^3)^3 : \nu^3 - 1.$$

We note that this relation considered as an equation for ν is not normal. This is one great disadvantage of the normal form $Y^2Z - YZ^2 = X^3 + 3\nu XYZ$. However this normal form degenerates in a much nicer way than the normal form $X^3 + Y^3 + Z^3 = 3\nu XYZ$ in the sense we shall explain later.

3. Fields of modular functions of low levels. Suppose that A is an elliptic curve whose absolute invariant $j(A)$ is a variable over a prime field F.

Consider a homomorphism of A onto another elliptic curve B. Since every homomorphism can be factored into homomorphisms of prime degrees, we can assume that the degree of the homomorphism is a prime number p. Also we can assume that p is different from the characteristic of F, for otherwise the situation will become trivial. Then the *transformation theory of elliptic functions* will answer to the following problems: (1) How is $j(B)$ related to $j(A)$? (2) What is the arithmetic nature of the homomorphism? First part is the transformation of the parameter space while the second part is the transformation of the entire fibre system of elliptic curves. At any rate the homomorphism is determined up to an isomorphism by its kernel, which is a cyclic subgroup of A of order p. We know that the points of A of order p form a finite Abelian group of type (p,p). Therefore we have $p+1$ distinct homomorphisms from A to another elliptic curves of which B is a member. This already suggests the importance of points of finite orders. In fact the Galois theory of these points is a necessary preliminary for the transformation theory. In this section we shall define the field of modular functions with level along this line and we shall investigate the special cases of level 2 and of level 3. We shall start by summarizing some of the well-known elementary properties of groups of two-by-two integer matrices modulo integers.

Let n be a non-negative integer different from 1. The case $n=0$ is exceptional. We shall denote the general linear group of two-by-two matrices over integers modulo n by $GL(2,n)$. Similarly the special linear group $SL(2,n)$ is defined. We shall use the following notation for the simplicity of the printing

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a\ b, c\ d).$$

The group $SL(2,n)$ contains the group Z consisting of $\pm(1\ 0, 0\ 1)$ in the center. The linear fractional group $LF(2,n)$ is defined as the corresponding factor group. We note that Z can reduce to the identity in case $n=2$ and only in this case. If n splits into a product of relatively prime natural numbers n' and n'', then $GL(2,n)$ and $SL(2,n)$ decomposes into direct products $GL(2,n')\times GL(2,n'')$ and $SL(2,n')\times SL(2,n'')$. Therefore, if $\phi(n)$ is the Euler function and if $\psi(n)$ denotes the number of cyclic subgroups of order n in the Abelian group of type (n,n), i.e., if we put

$$\psi(n) = n\cdot\prod_{p\mid n}(1+p^{-1}),$$

the orders of $GL(2,n)$, $SL(2,n)$ and $LF(2,n)$ can be expressed as $n\phi(n)^2\psi(n)$, $n\phi(n)\psi(n)$ and $\frac{1}{2}\cdot n\phi(n)\psi(n)$. Here the case $n=2$ is exceptional for $LF(2,n)$

and its order is equal to $n\phi(n)\psi(n)=6$. Moreover, if we exclude this case, the number of elements of order 2 in $SL(2,n)$ is smaller than the number of elements of order 2 in $LF(2,n)\times Z$. Hence $SL(2,n)$ does not split into this direct product. We also note that $(1\ 1,0\ 1)$ and $(1\ 0,1\ 1)$ generate $SL(2,0)$, hence $SL(2,n)$ in general. In this connection we note that the normal subgroup of $SL(2,0)$ of index 6 defined by $(a\ b,c\ d)\equiv(1\ 0,0\ 1)$ mod 2 is the direct product of Z and the subgroup of $SL(2,0)$ generated by $(1\ 2,0\ 1)$ and $(1\ 0,2\ 1)$, which is a free group. A similar situation prevails even if we take module 2^e with $e\geqq 2$. Also, if a subgroup of $SL(2,3^e)$ reduces to the whole $SL(2,3)$ modulo 3 and contains both $(1\ 3,0\ 1)$ and $(1\ 0,3\ 1)$, this group must be $SL(2,3^e)$ for $e\geqq 1$. A proof can be obtained by induction on e.

Let A be an elliptic curve defined over a field K. Let n be a natural number not divisible by the characteristic of K and let Ω be the group of points of A of order n. Then Ω is a finite Abelian group of type (n,n) and $K(\Omega)$ is a finite Galois extension of K. Moreover the Galois group of $K(\Omega)$ over K operates faithfully on Ω. Therefore the Galois group is mapped isomorphically into $GL(2,n)$ with reference to a base of Ω. As we know, if we denote by k_0 the field of n-th roots of unity defined over the prime field F, then $K(\Omega)$ always contains k_0. Moreover, if an automorphism of $K(\Omega)$ over K transforms n-th roots of unity to m-th powers, the determinant of its image in $GL(2,n)$ is congruent to m modulo n. In particular, if K contains k_0, the image of the Galois group in $GL(2,n)$ is contained in $SL(2,n)$. We note that these properties come from the existence of a skew-symmetric pairing of Ω to itself [16, 9]. We also note that the classical proof depends on the so-called Abel's relation [12, 15].

Now, suppose that the absolute invariant $j(A)$ of A is different from 0 and 12^3. Then A has only two automorphisms defined by $u\to\pm u$. This is clear from the consideration made in the previous section. Suppose next that A' is another elliptic curve, also defined over K, with $j(A')=j(A)$. Then, by the above remark, we have only two isomorphisms between A and A', which we can denote by α and $-\alpha$. In general α is not defined over K. However α is always defined over a separable extension of K. This is a consequence of a general theorem of Chow for Abelian varieties [2], and in the present case it can be proved elementarily using the results in the previous section. These being remarked, if we identify points u and $-u$ on A, we get a projective straight line D defined over K. We shall denote the identification mapping, also defined over K, by Ku. Suppose that D' is associated with A' as D is associated with A. Then we get a correspondence between D and D'

as follows: Let u be a generic point of A over K. Then $Ku(u)$ and $Ku(\pm \alpha u)$ are the corresponding generic points of D and D' over K. We note that $Ku(\pm \alpha u)$ has no other conjugate over $K(Ku(u))$ than itself. Moreover $Ku(\pm \alpha u)$ is separable over $K(Ku(u))$, hence $Ku(\pm \alpha u)$ is rational over $K(Ku(u))$. Since the situation is symmetric in A and A', we see that the correspondence between D and D' is an everywhere biregular mapping defined over K. As a consequence, if v and v' are the corresponding points of A and A' under one of the two isomorphisms between A and A', we always get $K(Ku(v)) = K(Ku(v'))$. This fact will be of constant use later.

Now, let j be a variable over the prime field F. Then we can find an elliptic curve A_j defined over $F(j)$ with $j(A_j) = j$. The most elementary proof can be obtained by just writing down equations for elliptic curves having j as absolute invariant. In case the characteristic is different from 2 and 3 we take

$$Y^2Z = 4X^3 - 3^3 j(j - 12^3)^{-1}(X + Z)Z^2$$

as A_j. In case the characteristic is 2 or 3 we take

$$Y^2Z - XYZ = j^{-1}X^3 + jZ^3, \qquad Y^2Z = X^3 - X^2Z + j^{-1}Z^3$$

accordingly as A_j [3]. These cubic curves are indeed non-singular, hence we can introduce group structures with reference to $(0, 1, 0)$. We note that these elliptic curves remain to be elliptic curves with j as absolute invariant provided j is different from 0, 12^3, ∞. We shall see later that elliptic curves like A_j must degenerate at $j = 0$, 12^3 and ∞ irrespective of its construction.

As before, let n be a natural number not divisible by the characteristic of F and let Ω be the group of points of A_j of order n. Then $F(j, \Omega)$ is a finite Galois extension of $F(j)$ and so is $F(j, Ku(\Omega))$. *This Galois extension of $F(j)$ is intrinsically defined by n*, i.e. it does not depend on the choice of A_j. We extend F to its algebraic closure k and we call $k(j, Ku(\Omega))$ the *field of modular functions of level n*. We note that $k(j, \Omega)$ is at most a quadratic extension of $k(j, Ku(\Omega))$. Also, if m is a natural number, the endomorphism $u \to m \cdot u$ of A_j gives rise to a natural projection of the field of modular functions of level mn to the field of modular functions of level n. We shall show that $k(\lambda)$ *and* $k(\mu)$ *are the fields of modular functions of level* 2 *and of level* 3. Here λ and μ correspond to j by the equations discussed in the previous section.

Let Ω be the group of points of A_j of order 2. We assume, of course, that the characteristic is different from 2. Then we have $F(j, Ku(\Omega)) = F(j, \Omega)$ and we can transform A_j to $\alpha \cdot Y^2Z = X(X - Z)(X - \lambda Z)$ over $F(j, \Omega)$.

Therefore $F(\lambda)$ is contained in $F(j,\Omega)$. However, since $[F(j,\Omega):F(j)]$ is at most equal to 6, we have $F(j,\Omega)=F(\lambda)$, hence $k(j,Ku(\Omega))=k(\lambda)$. Let Ω be, next, the group of points of A_j of order 3. We are automatically assuming that the characteristic is different from 3. Then we can transform A_j to $X^3+Y^3+Z^3=3\mu XYZ$ over $F(j,\Omega)$, hence $F(\mu,\rho)$ is contained in $F(j,\Omega)$. Here ρ is, as before, a primitive third root of unity. On the other hand, because of a property of Ku, we get $F(\mu,\rho)=F(\mu,Ku(\Omega))$, hence $F(j,Ku(\Omega))$ is contained in $F(\mu,\rho)$. Therefore we get the inclusion relation $F(j,Ku(\Omega))\subset F(\mu,\rho)\subset F(j,\Omega)$, hence by putting $k_0=F(\rho)$ we get $k_0(j,Ku(\Omega))\subset k_0(\mu)\subset k_0(j,\Omega)$. However $[k_0(j,\Omega):k_0(j,Ku(\Omega))]$ is at most equal to 2 and the Galois group of $k_0(\mu)$ over $k_0(j)$, which is the alternating group of permutations of four letters, does not contain any normal subgroup of order 2. Therefore we have $k_0(j,Ku(\Omega))=k_0(\mu)$, hence $k(j,Ku(\Omega))=k(\mu)$.

Now we shall examine the extensions $k(\lambda)$ and $k(\mu)$ of $k(j)$ more closely for our later purpose. Consider $k(\lambda)$ first assuming that the characteristic is different from 2. We know that $k(\lambda)$ is ramified over $k(j)$ at $j=0,12^3,\infty$ and nowhere else. Moreover in case the characteristic is different from 3 the ramification is tame and the corresponding inertia groups are cyclic of order 3, 2, 2. If the characteristic is 3, then $k(\lambda)$ is ramified only at $j=0$ and ∞. It is still tamely ramified at $j=\infty$ and the corresponding inertia groups are cyclic of order 2. However at $j=0$ the ramification is wild. There is only one point $\lambda=-1$ above $j=0$, hence the inertia group is the whole Galois group. Moreover, as we can see, the cyclic subgroup of order 3, necessarily consisting of transformations $\lambda\to\lambda$, $(1-\lambda)^{-1}$, $(\lambda-1)\lambda^{-1}$, is the first ramification group while the second ramification group reduces to the identity. The different of the covering is, therefore, given by $(0)+(1)+(\infty)+7.(-1)$. This agrees with the expression $dj=(1+\lambda)^7\lambda^{-3}(1-\lambda)^{-3}d\lambda$. Next consider $k(\mu)$ assuming that the characteristic is different from 3. We know that $k(\mu)$ is ramified over $k(j)$ at $j=0,12^3,\infty$ and nowhere else. Moreover in case the characteristic is different from 2 the ramification is tame and the corresponding inertia groups are cyclic of order 3, 2, 3. If the characteristic is 2, then $k(\mu)$ is ramified only at $j=0$ and ∞. It is still tamely ramified at $j=\infty$ and the corresponding inertia groups are cyclic of order 3. However at $j=0$ the ramification is wild. There is only one point $\mu=0$ above $j=0$, hence the inertia group is the whole Galois group. Moreover, as we can see, the Klein four group, necessarily consisting of transformations $\mu\to\mu$, $\zeta\mu(\mu-\zeta)^{-1}$ for $\zeta=1$, ρ, ρ', is the first ramification group while the second ramification group reduces to the identity. The different of the covering is,

therefore, given by $2.((1)+(\rho)+(\rho')+(\infty))+14.(0)$. This agrees again with the expression $dj=\mu^{14}(\mu^3-1)^{-4}d\mu$.

Finally we note that every tamely ramified extension of $k(j)$ ramified only at two points is cyclic. This follows at once from the *relative genus formula*, which is as follows: Let Σ be a finite covering of a curve K. Let g and g_0 be the genera of Σ and K; let $\mathfrak{d}$ be the different of the covering. Then we have $2g-2=\deg(\mathfrak{d})+[\Sigma:K](2g_0-2)$. On the other hand, as it was observed by Abhyankar [1], the field $k(j)$ can be covered by fields of "large Galois groups" ramified only at one point.

4. Degeneration and ramification. There is a close connection between degenerations of elliptic curves and ramifications of certain extensions of parameter fields. The examination of this connection will provide *key lemmas* for the Galois theory of points of finite orders. We shall start by examining degenerate members of the linear pencils of elliptic curves introduced in Section 2. Let F be, as before, a prime field of an arbitrary characteristic. In case the characteristic is different from 2 we consider the linear pencil defined over F by $Y^2Z=X(X-Z)(X-\lambda Z)$. This linear pencil contains three singular members which correspond to $\lambda=0,1,\infty$. The singular member which corresponds to $\lambda=\infty$ is a reducible cubic. However two other singular members are irreducible and the singular points $(0,0,1)$ for $\lambda=0$ and $(1,0,1)$ for $\lambda=1$ are what we call *ordinary double points*. In case the characteristic is different from 3 we consider the linear pencils defined over F by $X^3+Y^3+Z^3=3\mu XYZ$ and $Y^2Z-YZ^2=X^3+3\nu XYZ$. Both linear pencils contain four singular members which correspond to $\mu,\nu=1,\rho,\rho',\infty$. The singular members which correspond to $\mu=1,\rho,\rho',\infty$ and $\nu=\infty$ are all reducible cubics. However singular members which correspond to $\nu=1,\rho,\rho'$ are irreducible and the respective singular points $(1,1,-1)$, $(\rho',1,-1)$, $(\rho,1,-1)$ are again ordinary double points. In this connection we remark also that $Y^2Z=4X^3-3^3j(j-12^3)^{-1}(X+Z)Z^3$ reduces at $j=\infty$ to an irreducible cubic with an ordinary double point $(-\frac{3}{2},0,1)$. Similarly $Y^2Z=X^3-X^2Z+j^{-1}Z^3$ reduces at $j=\infty$ to an irreducible cubic with an ordinary double point at $(0,0,1)$. However $Y^2Z-XYZ=j^{-1}X^3+jZ^3$ will become reducible at $j=\infty$.

Consider in general an elliptic curve defined over a field K which is complete under a real discrete valuation. Let k be the residue field and let A' be the unique specialization of A over the natural homomorphism of the valuation ring of K onto k. We assume that A' is either non-singular or has one ordinary double point different from the image of the neutral element

of A. We also assume that k is algebraically closed. Let n be a natural number not divisible by the characteristic of k and let Ω be the group of points of A of order n. Then, *in case A' is non-singular we have $K(\Omega)=K$. In case A' has an ordinary double point Ω contains a base ω_1, ω_2 on which the Galois group of $K(\Omega)$ over K operates as follows*

$$\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\rightarrow\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}.$$

The cyclic group or order n generated by ω_2, which we called the *group of vanishing points of order n*, is uniquely determined by A. Here m is an integer modulo n. This we proved separately in a more general case of Jacobian varieties [7, 9].

Now, as before, take k to be the algebraic closure of F. Let j be a variable over k and consider A_j. Then, *no matter how we construct A_j, this must degenerate at least at $j=0$, 12^3 and ∞.* In fact, suppose that the characteristic is different from 2 and let Ω be the group of points of A_j of order 2. If (a) is a rational point of a projective straight line over k, we take the power-series field $k((j-a))$ as K and A_j as A. In this way, if A_a is non-singular, we see that $k(j, Ku(\Omega))=k(\lambda)$ is unramified over $k(j)$ at $j=a$. However we know that $k(\lambda)$ is ramified over $k(j)$ at $j=0$, 12^3 and ∞. Therefore A_j can not remain to be non-singular at these points. If the characteristic is 2, we consider the group Ω of points of A_j of order 3 and apply the fact that $k(j, Ku(\Omega))=k(\mu)$ is ramified over $k(j)$ at $j=0$ and ∞. On the other hand, let Ω_λ, Ω_μ and Ω_ν be the groups of points of order n on the elliptic curves $Y^2Z=X(X-Z)(X-\lambda Z)$, $X^3+Y^3+Z^3=3\mu XYZ$ and $Y^2Z-YZ^2=X^3+3\nu XYZ$. Then by a similar consideration we see that $k(\lambda, \Omega_\lambda)$ is ramified over $k(\lambda)$ only at $\lambda=0, 1, \infty$ and the ramification is tame at $\lambda=0, 1$. We see also that $k(\mu, \Omega_\mu)$ and $k(\nu, \Omega_\nu)$ are ramified over $k(\mu)$ and $k(\nu)$ respectively only at $\mu, \nu=1, \rho, \rho', \infty$ and $k(\nu, \Omega_\nu)$ is tamely ramified at $\nu=1, \rho, \rho'$. Moreover in case the ramification is tame the corresponding inertia groups are cyclic of an order which divides n. These local informations will play a definitive role in determining the Galois groups explicitly. There are some more things to be cleared up before we start discussing those Galois groups.

One thing to be remarked is that *$Y^2Z=X(X-Z)(X-\lambda Z)$ has only four rational points over $k(\lambda)$, and these are exactly points of order 2.* In fact, let v be a rational point of $Y^2Z=X(X-Z)(X-\lambda Z)$ over $k(\lambda)$ different from the base points $(0,1,0)$, $(0,0,1)$, $(1,0,1)$ and consider its locus C over k. Then $Y^2Z=X(X-Z)(X-\lambda Z)$ intersects with C at v

with unit multiplicity and extra intersections are among the three base points, which together with $v_0 = (\lambda, 0, 1)$ form the group of points of order 2. In fact the restriction of the linear pencil to C gives rise to a linear pencil on C. The "variable part" of a linear pencil is, in general, a prime rational divisor over the parameter field [cf. 17]. However, since v is a member of this variable part and since v is rational over $k(\lambda)$, we see that v itself is the variable part. It is clear that the "fixed part" consists of the above mentioned base points of the original linear pencil. Therefore, if we denote the X-axis by C_0, then $Y^2Z = X(X-Z)(X-\lambda Z)$ intersects with $C - \deg(C) \cdot C_0$ at $(v) - \deg(C) \cdot (v_0)$ modulo base points. However, since $C - \deg(C) \cdot C_0$ is a divisor of a function on the projective plane, by applying the so-called Abel theorem we see that v is a point of order 2. The only possibility is then $v = v_0$. This proves the assertion. In the same way we see that *$X^3 + Y^3 + Z^3 = 3\mu XYZ$ has nine rational points over $k(\mu)$, and these are exactly points of order 3.* Moreover *$Y^2Z - YZ^2 = X^3 + 3\nu XYZ$ has only three rational points over $k(\nu)$, and these are* $(0,1,0)$, $(0,1,1)$, $(0,0,1)$.

Another thing to be remarked is the following: We know that every elliptic curve, in particular A_j, can be transformed into the normal forms discussed in Section 2. We shall investigate smallest fields over which these transformations are possible. Assume first that the characteristic is different from 2. Then we can transform A_j to $\alpha \cdot Y^2Z = X(X-Z)(X-\lambda Z)$ over $F(\lambda)$. This α is not uniquely determined by A_j. At any rate, in order to get $Y^2Z = X(X-Z)(X-\lambda Z)$, we must introduce $\alpha^{\frac{1}{2}}$, i.e. we must possibly go through a quadratic extension of $F(\lambda)$. On the other hand the discussion in Section 2 shows that the six conjugates of $Y^2Z = X(X-Z)(X-\lambda Z)$ over $F(j)$ can not be transformed into each other over $F(\lambda)$. However, if we introduce κ and κ' by $\kappa^2 = \lambda$ and $(\kappa')^2 = 1 - \lambda$, then the twelve isomorphisms are all defined over $k_0(\kappa, \kappa')$. Here k_0 is the field of fourth roots of unity. The field $k_0(\kappa, \kappa')$ has another meaning. If x and y are the inhomogeneous co-ordinate functions of $Y^2Z = X(X-Z)(X-\lambda Z)$, the *addition theorem* of x can be obtained by an elementary analytic geometry and we get

$$x(u+v) = x(u)x(v)(\lambda - x(u)x(v))^2(x(u)y(v) + x(v)y(u))^{-2}.$$

Therefore, if Ω_λ is the group of points of $Y^2Z = X(X-Z)(X-\lambda Z)$ of order 4, we have $F(\lambda, \Omega_\lambda) = k_0(\kappa, \kappa')$. At any rate, if we fix A_j, although $\alpha^{\frac{1}{2}}$ is not unique, it determines a unique extension of $k_0(\kappa, \kappa')$. We know that α is an element of $F(\lambda)$. If λ' corresponds to j' at which A_j remains to be non-singular, certainly $\alpha(\lambda')$ is different from 0 and ∞. Now, if the characteristic is also different from 3 and if we take $Y^2Z = 4X^3 - 3^3 j(j-12^3)^{-1}(X+Z)Z^2$

as A_j, then A_j degenerates only at $j=0$, 12^3 and ∞. Therefore

$$((1-\lambda+\lambda^2)(1+\lambda)(1-2\lambda)(2-\lambda))^{\frac{1}{2}}$$

is one of the possible radicals to be introduced over $k_0(\kappa,\kappa')$ and we can show that this is exactly the radical we need. If the characteristic is 3 and if we take $Y^2Z=X^3-X^2Z+j^{-1}Z^3$ as A_j, then A_j degenerates only at $j=0$ and ∞. Therefore $(1+\lambda)^{\frac{1}{2}}$ is one of the possible radicals to be introduced over $k_0(\kappa,\kappa')$ and we can show again that this is the radical we need. Next, assume that the characteristic is different from 3. Let Ω be the group of points of A_j of order 3. Then we can transform A_j to $X^3+Y^3+Z^3=3\mu XYZ$ over $F(j,\Omega)$. In this case the twelve conjugates of $X^3+Y^3+Z^3=3\mu XYZ$ over $F(j)$ can be transformed into each other over $k_0(\mu)$. Here k_0 is now the field of third roots of unity. We know that $k_0(j,\Omega)=F(j,\Omega)$ is at most a quadratic extension of $k_0(\mu)$. If the characteristic is also different from 2 and if we take $Y^2Z=4X^3-3^3j(j-12^3)^{-1}(X+Z)Z^2$ as A_j, we can see that $(2\mu(8+\mu^3)(8+20\mu^3-\mu^6))^{\frac{1}{2}}$ is the radical to be introduced over $k_0(\mu)$. In other words $k_0(j,\Omega)$ is indeed a quadratic extension of $k_0(\mu)$ obtained by adjoining the above radical to it. If the characteristic is 2 and if we take $Y^2Z-XYZ=j^{-1}X^3+jZ^3$ as A_j, we see that $k_0(j,\Omega)$ is the quadratic extension of $k_0(\mu)$ obtained by adjoining a root θ of $\theta^2-\theta=\mu^{-3}$ to it. We note that $k_0(j,\Omega)$ is, in this case, ramified over $k_0(\mu)$ only at $\mu=0$. Moreover the inhomogeneous equation $y^2-y=x^3$ defines an elliptic curve in characteristic 2 with $j=0$ as its absolute invariant.

In connection with what we discussed above we remark also the following. Suppose that μ and ν correspond to the same j which we assume to be a variable over the field k_0 of the third roots of unity. Then the transformations between $X^3+Y^3+Z^3=3\mu XYZ$ and $Y^2Z-YZ^2=X^3+3\nu XYZ$ are defined over $k_0(\mu,\nu)$. In fact, since the twelve conjugates of $X^3+Y^3+Z^3=3\mu XYZ$ over $F(j)$ are transformed into each other over $k_0(\mu)$, hence over $k_0(\mu,\nu)$, we have only to show that a transformation is possible over $k_0(\mu,\nu)$ for some choice of μ and ν. However this we have shown explicitly in Section 2. The field $k_0(\mu,\nu)$ has another meaning. If Ω_ν is the group of points of $Y^2Z-YZ^2=X^3+3\nu XYZ$ of order 3, we have $F(\nu,\Omega_\nu)=k_0(\mu,\nu)$. At any rate $F(\nu,\Omega_\nu)=k_0(\nu,\Omega_\nu)$ is contained in $k_0(\mu,\nu)$ by what we have remarked above. On the other hand we know that only three members of Ω_ν are rational over $k_0(\nu)$ and $k_0(\mu,\nu)$ is of degree 3 over $k_0(\nu)$. Hence $F(\nu,\Omega_\nu)=k_0(\mu,\nu)$ is the only possibility we have.

5. **Galois theory of division points.** We are now completely prepared

to attack our main problem.[3] Suppose that F is, as before, a prime field of an arbitrary characteristic and k its algebraic closure. The moduli λ, μ, ν are assumed to correspond to the same j which is a variable over k. Let n be a natural number not divisible by the characteristic of F. Then the groups of points of order n on A_j, $Y^2Z = X(X-Z)(X-\lambda Z)$, $X^3+Y^3+Z^3 = 3\mu XYZ$ and $Y^2Z - YZ^2 = X^3 + 3\nu XYZ$ will be denoted by Ω, Ω_λ, Ω_μ and Ω_ν. Also points of exact order n will be called primitive n-th division points.

We shall first discuss the case where the characteristic is different from 2. Then we have $k(\lambda, Ku(\Omega_\lambda)) = k(\lambda, Ku(\Omega))$ and both $k(\lambda)$ and $k(j, Ku(\Omega))$ are normal over $k(j)$, hence $k(\lambda, Ku(\Omega_\lambda))$ is normal over $k(j)$. On the other hand we know that $k(\lambda, \Omega_\lambda)$ is ramified over $k(\lambda)$ only at $\lambda = 0$, 1 and ∞. Since these points are conjugate over $k(j)$, we conclude that the inertia groups of $k(\lambda, Ku(\Omega_\lambda))$ over $k(\lambda)$ are conjugate in the Galois group of $k(\lambda, Ku(\Omega_\lambda))$ over $k(j)$. We also know that the orders of inertia groups of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ at $\lambda = 0$ and $\lambda = 1$ divide n. Therefore the order of the inertia groups of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ at $\lambda = \infty$ is, at any rate, a divisor of $2n$. Hence $k(\lambda, \Omega_\lambda)$ is tamely ramified over $k(\lambda)$. As a consequence, if n splits into relatively prime factors n' and n'', the field $k(\lambda, n''\cdot\Omega_\lambda)$ of n'-th division points and the field $k(\lambda, n'\cdot\Omega_\lambda)$ of n''-th division points are linearly disjoint over $k(\lambda)$. Otherwise their intersection Σ will be a proper Galois extension of $k(\lambda)$ which is tamely ramified over $k(\lambda)$. Moreover Σ can be ramified over $k(\lambda)$ only at $\lambda = \infty$. This is a contradiction.

Let therefore n be a power of a prime number p. Assume first that p is odd. Let ω be a primitive n-th division point in Ω_λ. Then we can find an inertia group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ at $\lambda = 0$ or at $\lambda = 1$ under which ω is transformed into n distinct conjugates. Otherwise $n/p\cdot\omega$ will be kept invariant by all inertia groups of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ at $\lambda = 0$ and $\lambda = 1$, i.e. the subextension $k(\lambda, n/p\cdot\omega)$ of $k(\lambda, \Omega_\lambda)$ will be unramified over $k(\lambda)$ at $\lambda = 0$ and $\lambda = 1$. This implies that $n/p\cdot\omega$ is rational over $k(\lambda)$. However this is not possible, because p is odd. Therefore we can find an inertia group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ and the corresponding base ω_1, ω_2 of Ω_λ such that the inertia group operates on this base as $(\omega_1, \omega_2) \to (\omega_1 + m\omega_2, \omega_2)$ for $m = 1, \cdots$. In the same way we can find another inertia group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ which operates as $(\omega_2, \omega_1 + c\omega_2) \to (\omega_2 + m(\omega_1 + c\omega_2), \omega_1 + c\omega_2)$ for $m = 1, \cdots$. Here, by replacing ω_1 by $\omega_1 - c\omega_2$, we can assume that we have $c = 0$ from the beginning. Then the Galois group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ contains two

[3] If the reader is interested only in the field of modular functions with level, he can skip over some preparations and also some argument in this section.

substitutions of the form $(1\ 1, 0\ 1)$ and $(1\ 0, 1\ 1)$ both modulo n. However these substitutions generate the whole $SL(2,n)$. Therefore, by the previous remark, if n is just an odd natural number, the Galois group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ is $SL(2,n)$.[4] Consequently the Galois group of $k(\lambda, Ku(\Omega_\lambda))$ over $k(\lambda)$ is $LF(2,n)$. Since, in general the Galois group of $k(j, Ku(\Omega))$ over $k(j)$ is at most $LF(2,n)$, this group is also $LF(2,n)$. In particular $k(\lambda)$ and $k(j, Ku(\Omega))$ are linearly disjoint over $k(j)$. Moreover the Galois group of $k(j,\Omega)$ over $k(j)$ must be $SL(2,n)$. Otherwise we have $k(j,\Omega) = k(j, Ku(\Omega))$, hence $k(\lambda, \Omega_\lambda)$ is a quadratic extension of $k(\lambda, Ku(\Omega_\lambda)) = k(\lambda, Ku(\Omega)) = k(\lambda, \Omega)$. Therefore the quadratic extension of $k(\lambda)$ over which A_j can be transformed into $Y^2Z = X(X-Z)(X-\lambda Z)$ is contained in $k(\lambda, \Omega_\lambda)$, hence $k(\lambda, \Omega_\lambda)$ will be the compositum of $k(\lambda, Ku(\Omega_\lambda))$ and this quadratic extension over $k(\lambda)$. This is a contradiction, because $SL(2,n)$ does not split into the direct product of $LF(2,n)$ and Z.

Next, consider the case $p = 2$. As before, we can find a base ω_1, ω_2 of Ω_λ such that one inertia group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ operates on this base as $(\omega_1, \omega_2) \to (\omega_1 + 2m\omega_2, \omega_2)$ for $m = 1, \cdots$ and another inertia group operates as $(\omega_2, \omega_1) \to (\omega_2 + 2m\omega_1, \omega_1)$ for $m = 1, \cdots$. Then the Galois group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ contains two substitutions of the form $(1\ 2, 0\ 1)$ and $(1\ 0, 2\ 1)$ both modulo n. Hence the Galois group of $k(\lambda, Ku(\Omega_\lambda))$ over $k(\lambda)$ contains the normal subgroup of $LF(2,n)$ of index 6 whose elements are represented by $(a,b,c,d) \equiv (1\ 0, 0\ 1) \bmod 2$. Therefore, because of the relation $k(j, Ku(\Omega)) = k(\lambda, Ku(\Omega))$, the Galois group of $k(\lambda, Ku(\Omega_\lambda)) = k(\lambda, Ku(\Omega))$ over $k(\lambda)$ is exactly that group and the Galois group of $k(j, Ku(\Omega))$ over $k(j)$ is the whole $LF(2,n)$. On the other hand, in this case, we have $k(\lambda, \Omega_\lambda) = k(\lambda, Ku(\Omega_\lambda))$. Otherwise n is at least equal to 4 and the Galois group of $k(\lambda, \Omega_\lambda)$ over $k(\lambda)$ will contain the substitution which transforms every element of Ω_λ to its inverse. The same situation must prevail for $n/4 \cdot \Omega_\lambda$. However we know that the field $k(\lambda, n/4 \cdot \Omega_\lambda)$ of fourth division points is an extension of $k(\lambda)$ of degree 4, hence we get $k(\lambda, n/4 \cdot \Omega_\lambda) = k(\lambda, Ku(n/4 \cdot \Omega_\lambda))$. This is a contradiction, hence the assertion is proved. However, if we exclude the case $n = 2$, then $k(j,\Omega)$ is a quadratic extension of $k(j, Ku(\Omega))$. In fact, let Σ be the quadratic extension of the field of fourth division points over which A_j can be transformed into $Y^2Z = X(X-Z)(X-\lambda Z)$. Then $\Sigma(\Omega_\lambda) = \Sigma(\Omega)$ is a quadratic extension of $k(\lambda, \Omega_\lambda)$, as it is clear from the consideration in the previous section, and its non-identical automorphism transforms every element of Ω to its inverse. This proves the assertion.

[4] The original argument of the author was a little bit more complicated. A simplification was made through a discussion with Professor Tamagawa in the Fall of 1957.

Since we know that the Galois group of $k(j, Ku(\Omega))$ over $k(j)$ is $LF(2,n)$, the Galois group of $k(j,\Omega)$ over $k(j)$ is $SL(2,n)$. We can summarize some of our results as follows:[6]

THEOREM 1. *Let λ be transcendental over a prime field F of characteristic different from 2. Let n be a natural number not divisible by the characteristic and let Ω_λ be the group of points of $Y^2Z = X(X-Z)(X-\lambda Z)$ of order n. Then $F(\lambda,\Omega_\lambda)$ contains the field k_0 of n-th roots of unity and k_0 is algebraically closed in $k_0(\lambda,\Omega_\lambda)$. Moreover the Galois group of $k_0(\lambda,\Omega_\lambda)$ over $k_0(\lambda)$ is the subgroup of $SL(2,n)$ defined by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \bmod 4.$$

It might not be necessary, but, to make sure, we shall explain why the theorem for k_0 follows from the above consideration for k. We know that $F(\lambda,\Omega_\lambda)$ contains k_0. Also we can see quite easily that the Galois group of $k_0(\lambda,\Omega_\lambda)$ over $k_0(\lambda)$ is, at any rate, a subgroup of the group in the theorem, which is the Galois group of $k(\lambda,\Omega_\lambda)$ over $k(\lambda)$. Therefore these two Galois groups must be the same. In other words $k_0(\lambda,\Omega_\lambda)$ and $k(\lambda)$ are linearly disjoint over $k_0(\lambda)$, hence $k_0(\lambda,\Omega_\lambda)$ is a regular extension of k_0.

Next we shall consider the case of characteristic 2 or, more generally, the case where the characteristic is different from 3. We can assume that the moduli μ and ν are related by $(\mu^3-1)(\nu^3-1)=1$. Then $k(\mu)$ and $k(\nu)$ are linearly disjoint cyclic extensions of degree 3 over $k(\mu^3)=k(\nu^3)$. We shall show that $k(\mu,\Omega_\mu)$ and $k(\nu,\Omega_\nu)$ are tamely ramified over $k(\mu)$ and over $k(\nu)$. We know that $k(\nu,\Omega_\nu)$ is tamely ramified over $k(\nu)$ at $\nu=1,\rho,\rho'$. Therefore $k(\mu,\nu,\Omega_\mu)=k(\mu,\nu,\Omega_\nu)$ is tamely ramified over $k(\mu,\nu)$ at $\mu=\infty$. Since the characteristic is different from 3, it is also tamely ramified over $k(\mu)$ at $\mu=\infty$. Since the twelve conjugates of $X^3+Y^3+Z^3=3\mu XYZ$ over $k(j)$ are transformable into each other over $k(\mu)$, we conclude that $k(\mu,\Omega_\mu)$ is normal over $k(j)$. Since the Galois group of $k(\mu,\Omega_\mu)$ over $k(j)$ operates transitively on $\mu=1,\rho,\rho',\infty$, the inertia groups of $k(\mu,\Omega_\mu)$ over $k(\mu)$ are conjugate in this Galois group. In particular $k(\mu,\Omega_\mu)$ is tamely ramified over $k(\mu)$. Hence going backwards we see that $k(\nu,\Omega_\nu)$ is also tamely ramified over $k(\nu)$ as asserted. Since the orders of the inertia groups of $k(\nu,\Omega_\nu)$ over $k(\nu)$ at $\nu=1,\rho,\rho'$ divide n, if n splits into relatively prime factors n' and n'', the field $k(\nu,n''\cdot\Omega_\nu)$ of n'-th division points and the field $k(\nu,n'\cdot\Omega_\nu)$ of n''-th

[6] The special case of this theorem in the case of characteristic zero and for odd n was proved by Kronecker using general transformation formulas of Gauss-Jacobi theta functions [12, 13]. For a systematic treatment, see [15].

division points are linearly disjoint over $k(\nu)$. Moreover, if we compare $k(\mu,\Omega_\mu)$ with $k(\nu,\Omega_\nu)$ over $k(\mu^3)=k(\nu^3)$ at $\mu=\infty$, we can see that the order of the inertia groups of $k(\mu,\Omega_\mu)$ over $k(\mu)$ at $\mu=\infty$, hence also at $\mu=1,\rho,\rho'$, divide n. Therefore, as above, the splitting of n into relatively prime factors results in the splitting of $k(\mu,\Omega_\mu)$ into linearly disjoint subextensions over $k(\mu)$.

Let therefore n be a power of a prime number p. Assume first that p is different from 3. Then, as before, we can conclude that the Galois groups of $k(\mu,\Omega_\mu)$ and $k(\nu,\Omega_\nu)$ over $k(\mu)$ and $k(\nu)$ are isomorphic to $SL(2,n)$. The same situation prevails provided n is not divisible by 3. This implies that the Galois group of $k(j,Ku(\Omega))$ over $k(j)$ is $LF(2,n)$ and, as before, that the Galois group of $k(j,\Omega)$ over $k(j)$ is $SL(2,n)$. Next, consider the case $p=3$. Then, since it is so for $n=3$, we have $k(\mu,\Omega_\mu)=k(\mu,Ku(\Omega_\mu))$ in general. Moreover, by a similar consideration as before, we see that the Galois group of $k(\mu,\nu,\Omega_\mu)=k(\mu,\nu,\Omega_\nu)$ over $k(\mu,\nu)$ contains two substitutions of the form $(1\ 3,0\ 1)$ and $(1\ 0,3\ 1)$ both modulo n. Therefore the Galois group of $k(\mu,\Omega)=k(j,\Omega)$ over $k(j)$ also contains these substitutions, hence it must be the whole $SL(2,n)$. Consequently the Galois group of $k(j,Ku(\Omega))$ over $k(j)$ is $LF(2,n)$. This implies immediately that the Galois group of $k(\mu,\Omega_\mu)$ over $k(\mu)$ is the normal subgroup of $SL(2,n)$ of index 24 defined by $(a\ b,c\ d)\equiv(1\ 0,0\ 1)$ mod 3. We can summarize some of our results as follows:

THEOREM 2. *Let μ be transcendental over a prime field F of characteristic different from 3. Let n be a natural number not divisible by the characteristic and let Ω_μ be the group of points of $X^3+Y^3+Z^3=3\mu XYZ$ of order n. Then $F(\mu,\Omega_\mu)$ contains the field k_0 of n-th roots of unity and k_0 is algebraically closed in $k_0(\mu,\Omega_\mu)$. Moreover the Galois group of $k_0(\mu,\Omega_\mu)$ over $k_0(\mu)$ is the subgroup of $SL(2,n)$ defined* by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 3.$$

Moreover, if we understand by A_j the plane cubics introduced in Section 3, we can state the following theorem:

THEOREM 3. *Let j be transcendental over a prime field F of an arbitrary characteristic. Let n be a natural number not divisible by the characteristic and let Ω be the group of points of A_j of order n. Then $F(j,\Omega)$ contains the field k_0 of n-th roots of unity and k_0 is algebraically closed in $k_0(j,\Omega)$. Moreover the Galois group of $k_0(j,\Omega)$ over $k_0(j)$ is $SL(2,n)$ and the Galois*

group of $F(j,\Omega)$ *over* $F(j)$ *consists of elements of* $GL(2,n)$ *whose determinants give rise to the well-known automorphisms of* k_0 *over* F.

The last statement requires some explanation. Any automorphism of $F(j,\Omega)$ over $F(j)$ can be represented, with reference to a base of Ω, by an element $(a\ b, c\ d)$ of $GL(2,n)$. The theorem asserts that this automorphism transforms each n-th root of unity into its $(ad-bc)$-th power. If the characteristic is zero, there is no condition. However, if the characteristic is positive, this means that $ad-bc$ is congruent to a power of the characteristic modulo n. At any rate, if an element of $GL(2,n)$ satisfies this condition, it appears as an automorphism of $F(j,\Omega)$ over $F(j)$. We note that exactly the same statement can also be added to Theorem 1 and Theorem 2.

On the other hand, if we fix a prime number p different from the characteristic of F and if we denote by Ω the p-primary part of the group of points of A_j of finite orders, the algebraic closure k_0 of F in $F(j,\Omega)$ is the field of all p^e-th roots of unity for $e=1,\cdots$. Moreover the Galois group of $k_0(j,\Omega)$ over $k_0(j)$ with Krull's topology is the special linear group of two-by-two matrices over the ring of Hensel's p-adic integers.

6. Fields of modular functions. The field of modular functions of level n was introduced in Section 3 as follows: Let k be the algebraic closure of the prime field F of characteristic not dividing n. Let j be transcendental over k and let Ω be the group of points of A_j of order n. Then $k(j,Ku(\Omega))$ is the field in question. In the previous section we determined the Galois group of $k(j,Ku(\Omega))$ over $k(j)$, i.e. we proved the following theorem:

THEOREM 4. *The Galois group of the field of modular functions of level* n *over* $k(j)$ *is* $LF(2,n)$.

For $n=3$ the Galois group is called the *tetrahedral group.* As we know, the tetrahedral group is just the alternating group of permutations of four letters. Similarly for $n=5$ the Galois group is called the *icosahedral group.* This is the first simple group in this sequence of groups and it is the alternating group of permutations of five letters. As we shall see presently, the genus of the field $k(j,Ku(\Omega))$ is zero up to $n=5$ and hence, in the case of characteristic zero, the Galois group is represented as a group of rotations of a sphere, which gives rise to a polyhedral decomposition of the sphere. This is why the Galois groups have such geometric names.

THEOREM 5. *The genus* g *of the field of modular functions of level* n *is given by*

$$2g-2=1/12\cdot(n-6)\phi(n)\psi(n).$$

Here the case $n=2$ is exceptional and, in that case, we just get $g=0$.

First we note that the ramification index of $k(j,Ku(\Omega))$ over $k(j)$ at $j=\infty$ is n. In case the characteristic is different from 2, by the remark in Section 4, we know that the ramification index is a divisor of n. Suppose that n is even. Then $k(j,Ku(\Omega))$ contains $k(\lambda)$ and the ramification index of $k(\lambda,Ku(\Omega))$ over $k(\lambda)$ at $\lambda=0$, say, is $n/2$ while the ramification index of $k(\lambda)$ over $k(j)$ at $j=\infty$ is 2, whence the assertion. Suppose next that n is odd. Then the ramification index of $k(j,Ku(\Omega))$ over $k(j)$ at $j=\infty$ is at least equal to n, whence it must be equal to n. In the case of characteristic 2 we can conclude as follows. We know that the ramification index of $k(\nu,Ku(\Omega))$ over $k(\nu)$ at $\nu=1$, say, is n while $\nu=1$ covers $j=\infty$ only once. Therefore the ramification index of $k(j,Ku(\Omega))$ over $k(j)$ at $j=\infty$ must be n. This completes the proof. As a consequence the ramification is always tame at $j=\infty$. Next we shall determine other ramifications. Suppose that the characteristic is different from 2. Then $k(\lambda,Ku(\Omega))$ is ramified over $k(j)$ only at $j=0$, 12^3 and ∞, hence $k(j,Ku(\Omega))$ can be ramified over $k(j)$, besides $j=\infty$, only at $j=0$ and $j=12^3$. Moreover, if the characteristic is also different from 3, the ramification indices of $k(\lambda,Ku(\Omega))$ over $k(j)$ at $j=0$ and $j=12^3$ are 3 and 2. Therefore the ramification indices of $k(j,Ku(\Omega))$ over $k(j)$ at $j=0$ and $j=12^3$ divide 3 and 2. In particular $k(j,Ku(\Omega))$ is tamely ramified over $k(j)$. Therefore, if we remark that the Galois group is non-commutative, the ramification must take place at least at three points. Hence $k(j,Ku(\Omega))$ is ramified over $k(j)$ at $j=0$ and $j=12^3$ with respective ramification indices 3 and 2. Then by computing the degree of the divisor (dj) in $k(j,Ku(\Omega))$ we get the genus formula in this case. If the characteristic is 3, the ramification takes place only at $j=0$ and $j=\infty$, hence the ramification is wild at $j=0$. We shall show that the ramification index at $j=0$ is 6. We know that the inertia group of $k(\lambda,Ku(\Omega))$ over $k(j)$ at $j=0$ is the same as the inertia group of $k(\lambda)$ over $k(j)$ at $j=0$. Since this group contains only one non-trivial normal subgroup, which is of index 2, if the ramification index is not 6, it must be 2. Then the ramification is tame at $j=0$, but this is a contradiction. Once we know that the inertia group of $k(j,Ku(\Omega))$ over $k(j)$ at $j=0$ is the same as the inertia group of $k(\lambda)$ over $k(j)$ at $j=0$, we get the same genus formula as before. Finally, the case of characteristic 2 can be treated similarly through the field $k(\mu,Ku(\Omega))$. We see that $k(j,Ku(\Omega))$ is ramified over $k(j)$ only at $j=0$ and $j=\infty$, the ramification being wild at

$j=0$. We know that the inertia group of $k(\mu, Ku(\Omega))$ over $k(j)$ at $j=0$ is the same as the inertia group of $k(\mu)$ over $k(j)$ at $j=0$. Since this group contains only one non-trivial normal subgroup, which is of index 3, if the ramification index is not 12, it must be 3. Then the ramification is tame at $j=0$, and we get a contradiction. Therefore the inertia group of $k(j, Ku(\Omega))$ over $k(j)$ at $j=0$ must be the same as the inertia group of $k(\mu)$ over $k(j)$ at $j=0$. Hence again we get exactly the same genus formula.

In the course of the proof of Theorem 5 we also proved the following theorem:

THEOREM 6. *The field of modular functions of level n is ramified over $k(j)$ only at $j=0$, 12^3 and ∞. The ramification is always tame at $j=\infty$ with n as its index. If the characteristic is different from 2 and 3, it is tamely ramified at $j=0$ and $j=12^3$ with respective indices 3 and 2. If the characteristic is 3, it is wildly ramified at $j=0$ with the symmetric group of permutations of three letters as its inertia group and with the alternating group as the first ramification group; the second ramification group reduces to the identity. If the characteristic is 2, it is wildly ramified at $j=0$ with the tetrahedral group as its inertia group and with the Klein four group as the first ramification group; the second ramification group reduces to the identity.*

The Theorem 4 and the Theorem 6 are fundamental in the theory of modular functions with level. We can, for instance, calculate genera of all fields in between $k(j, Ku(\Omega))$ and $k(j)$ with the aid of *Hilbert's Galois theory* [6]. We shall illustrate this calculation by a special but important case of the *field of invariant transformation equation* of degree n. This field, say Σ, is defined to be the field which corresponds to the subgroup, say Π, of $LF(2,n)$ whose elements are represented by $(a\ b, c\ d)$ with $c \equiv 0 \bmod n$. We note that this field is of degree $\psi(n)$ over $k(j)$ and it is determined up to a conjugacy in $k(j, Ku(\Omega))$.

THEOREM 7. *The genus g of the field of invariant transformation equation of degree n is given by*[6]

$$2g-2 = 1/6 \cdot \psi(n) - 1/2 \cdot \pi_2(n) - 2/3 \cdot \pi_3(n) - \sum_{mm'=n} \phi((m, m')).$$

[6] In the case of characteristic zero and for a prime level p we find this formula already in Klein [10]. We note that $g+1$ is then the number of non-isomorphic elliptic curves in characteristic p having no point of order p except the neutral element [4, 8]. Furthermore $g+1$ is also the number of "new" finite singularities which the invariant transformation equation of degree p acquires by reduction modulo p.

Here $\pi_2(n)$ and $\pi_3(n)$ are the numbers of incongruent solutions of $x^2+1\equiv 0$ and $x^2+x+1\equiv 0$ both modulo n. Therefore $\pi_2(n)$ is zero if n is a multiple of 4; otherwise we have

$$\pi_2(n)=\prod_{p\mid n}(1+(-4/p)).$$

Similarly $\pi_3(n)$ is zero if n is a multiple of 9; otherwise we have

$$\pi_3(n)=\prod_{p\mid n}(1+(-3/p)).$$

Since the theorem is true for $n=2$, we shall assume that n is greater than 2. If we decompose $LF(2,n)$ into left cosets by H, the coset space can be identified with "projective line" over integers modulo n. This space is a homogeneous space with $LF(2,n)$ as structure group and with H as isotropy group. Suppose that T is an inertia group of $k(j,Ku(\Omega))$ over $k(j)$ at $j=a$. Then T operates on this homogeneous space, hence the space splits into several orbits such that, of course, each orbit is a homogeneous space with T as structure group. We call an orbit to be exceptional if the order of the corresponding isotropy group, which we call the multiplicity of the orbit, is greater than 1. According to Hilbert's Galois theory, there is a one-to-one correspondence between orbits and prime divisors of Σ lying above $j=a$. Moreover a prime divisor of Σ will be ramified in $k(j,Ku(\Omega))$ with index e if and only if the corresponding orbit has multiplicity e. Now in case $a=\infty$ the cyclic group of order n generated by $\pm(1\ 1,0\ 1)$ can be taken as T. Then, if we decompose n in the form mm', a point of our "projective line" having m as its second co-ordinate belongs to an orbit of multiplicity $m(m,m')$. Moreover the number of orbits of this type is $\phi((m,m'))$. Therefore, if $\mathfrak{d}$ is the different of $k(j,Ku(\Omega))$ over Σ, the contribution to $\deg(\mathfrak{d})$ of the prime divisors of $k(j,Ku(\Omega))$ lying above $j=\infty$ is given by

$$\sum_{mm'=n}\phi((m,m'))(1-1/m(m,m'))\cdot 1/2\cdot n\phi(n)$$
$$=(\sum_{mm'=n}\phi((m,m'))-\psi(n)/n)\cdot 1/2\cdot n\phi(n).$$

In order to determine contributions of other prime divisors, we observe the following. Consider an inertia group T of $k(j,Ku(\Omega))$ over $k(j)$ at $j=12^3$. Then elements of order 2 in T are conjugate to $\pm(0\ -1,1\ 0)$ in $LF(2,n)$. Similarly elements of order 3 in an inertia group of $k(j,Ku(\Omega))$ over $k(j)$ at $j=0$ are conjugate to either $\pm(-1\ -1,1\ 0)$ or $\pm(0\ 1,-1\ -1)$ in $LF(2,n)$. Since the proofs are similar, we shall prove the first statement. As we can see, it is sufficient to prove the statement for the direct limit of

all $k(j, Ku(\Omega))$. This case is, then, reduced to its p-primary part whose Galois group is the inverse limit of $LF(2, p^e)$ for $e = 1, \cdots$, i.e. the group of linear fractional transformations $x \to (ax + b)(cx + d)^{-1}$. Here a, b, c, d are p-adic integers satisfying $ad - bc = 1$. An element of order 2 of this group is then of the form $x \to (ax + b)(cx - a)^{-1}$ with $a^2 + bc + 1 = 0$. However an elementary number theory shows that this element is conjugate to $x \to -1/x$ in this group. As a consequence, in the case of characteristic 3, the whole inertia group of $k(j, Ku(\Omega))$ over $k(j)$ at $j = 0$ can not be contained in H. Also, in the case of characteristic 2, the Klein four group in the inertia group of $k(j, Ku(\Omega))$ over $k(j)$ at $j = 0$ can not be contained in H. Therefore, in every case, the multiplicities of exceptional orbits above $j = 12^3$ and $j = 0$ are 2 and 3. If the characteristic is different from 2 and 3, we have $\pi_2(n)$ exceptional orbits of multiplicity 2 and $\pi_3(n)$ exceptional orbits of multiplicity 3. If the characteristic is 3, we still have $\pi_2(n)$ exceptional orbits of multiplicity 2 but $1/2 \cdot \pi_3(n)$ exceptional orbits of multiplicity 3. Similarly, if the characteristic is 2, we have $1/2 \cdot \phi_2(n)$ exceptional orbits of multiplicity 2 and $\pi_3(n)$ exceptional orbits of multiplicity 3. However, just because of the wildness of ramification in the second and the third cases, the contributions to $\deg(\mathfrak{d})$ are the same in these three cases, and we get $(1/2 \cdot \pi_2(n) + 2/3 \cdot \pi_3(n)) \cdot 1/2 \cdot n\phi(n)$. If we sum up the contributions to $\deg(\mathfrak{d})$ in the relative genus formula

$$1/12 \cdot (n - 6)\phi(n)\psi(n) = \deg(\mathfrak{d}) + 1/2 \cdot n\phi(n)(2g - 2),$$

we get the genus formula stated in the theorem.

In the course of the above proof we considered the direct limit of fields of modular functions of levels $p, p^2, \cdots$ and its Galois group over $k(j)$ with Krull's topology, which is the group of linear fractional transformations

$$x \to (ax + b)(cx + d)^{-1}$$

with p-adic integer coefficients a, b, c, d satisfying $ad - bc = 1$. This we call the p-primary part of the *abstract modular group.*

Finally we shall explain the meaning of the field Σ. Suppose that ω is a primitive n-th division point of A_j. Here n is not a multiple of the characteristic. Then ω generates a cyclic subgroup $g(\omega)$, say, of A_j of order n. This cyclic group contains $\phi(n)$ primitive n-th division points by which we can construct a cycle $c(\omega)$. We note that $g(\omega)$ and $c(\omega)$ determine each other uniquely. The set of all primitive n-th division points of A_j is divided into $\psi(n)$ cycles like $c(\omega)$ with disjoint supports. If Ω is, as before, the group of points of A_j of order n, then $k(j, c(\omega))$ is a subfield of $k(j, Ku(\Omega))$.

Moreover the subgroup of $LF(2,n)$ which corresponds to this subfield is contained in H. Since $c(\omega)$ has at most $\psi(n)$ conjugates over $F(j)$, hence over $k(j)$, we see that it has exactly $\psi(n)$ conjugates over $k(j)$ and that the Galois group of $k(j,Ku(\Omega))$ over $k(j,c(\omega))$ is H. In other words we have $\Sigma=k(j,c(\omega))$. On the other hand the factor group $A_j/g(\omega)$ is an elliptic curve defined over $F(j,c(\omega))$. Therefore the corresponding absolute invariant j_ω is contained in $F(j,c(\omega))$. However, since $c(\omega)$ is separable over $F(j,j_\omega)$ and has no other conjugate than itself over $F(j,j_\omega)$, we see that it is rational over this field. In other words we have $F(j,j_\omega)=F(j,c(\omega))$. Moreover, since we have

$$[F(j,j_\omega):F(j)]=[k(j,j_\omega):k(j)]=\psi(n),$$

we see that $F(j,j_\omega)$ is a regular extension of F. Therefore, if $\Phi(j_\omega,j)=0$ is an irreducible equation over F, then $\Phi_n(X,Y)$ is *absolutely irreducible.* The equation $\Phi_n(X,Y)=0$ is what we call the *invariant transformation equation* of degree n. If we adjoin one root of $\Phi_n(X,j)=0$ to $k(j)$, we get the field Σ. If we adjoin all roots to $k(j)$, we get a subfield of $k(j,Ku(\Omega))$. The above consideration shows that the subgroup of $LF(2,n)$ which corresponds to this subfield is the group of scalar matrices in $SL(2,n)$ modulo Z. Therefore, over this splitting field of $\Phi_n(X,j)=0$ the field of modular functions of level n is composed of quadratic extensions the number of which is the half of the number of incongruent solutions of $x^2\equiv 1 \bmod n$.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] S. Abhyankar, "Coverings of algebraic curves," *American Journal of Mathematics*, vol. 79 (1957), pp. 825-856.

[2] W. L. Chow, "Abelian varieties over function fields," *Transactions of the American Mathematical Society*, vol. 78 (1955), pp. 253-275.

[3] M. Deuring, "Invarianten und Normalformen elliptischer Funktionenkörper," *Mathematische Zeitschrift*, vol. 47 (1941), pp. 47-56.

[4] ———, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität*, vol. 14 (1941), pp. 197-272.

[5] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper," I, *Journal für die reine und angewandte Mathematik*, vol. 175 (1936), pp. 55-62; II, *ibid.*, pp. 69-88; III, *ibid.*, pp. 193-208.

[6] D. Hilbert, "Die Theorie der algebraischen Zahlkörper," *Jahresbericht der Deutschen Mathematiker Vereinigung*, vol. 4 (1897), pp. 177-546.

[7] J. Igusa, "Fibre systems of Jacobian varieties," I, *American Journal of Mathematics*, vol. 78 (1956), pp. 171-199; II, *ibid.*, pp. 745-760.

[8] ———, "Class number of a definite quaternion with prime discriminant," *Proceedings of the National Academy of Sciences*, vol. 44 (1958), pp. 312-314.

[9] ———, "Abstract vanishing cycle theory," *Proceedings of the Japan Academy*, vol. 34 (1958), pp. 589-593.

[10] F. Klein, "Ueber die Transformation der elliptischen Funktionen und die Auflösung der Gleichungen fünften Grades," 1878-79, *Collected Works*, vol. 3 (1923), pp. 13-75.

[11] ———, "Zur Theorie der elliptischen Modulfunktionen," 1879, *Collected Works*, vol. 3 (1923), pp. 169-178.

[12] L. Kronecker, "Ueber die algebraischen Gleichungen, von denen die Theilung der elliptischen Functionen abhängt," 1875, *Collected Works*, vol. 4 (1929), pp. 261-273.

[13] ———, "Zur Theorie der elliptischen Functionen," 1883-89, *Collected Works*, vol. 4 (1929), pp. 345-495.

[14] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of basic field," *American Journal of Mathematics*, vol. 77 (1955), pp. 134-176.

[15] H. Weber, *Lehrbuch der Algebra*, III, Braunschweig (1908).

[16] A. Weil, *Variétés Abéliennes et courbes algébriques*, Paris (1948).

[17] O. Zariski, *Algebraic surfaces*, New York (1948).

A THEOREM OF COMPLETENESS OF CHARACTERISTIC SYSTEMS OF COMPLETE CONTINUOUS SYSTEMS.*

By K. KODAIRA and D. C. SPENCER.[1]

Dedicated to Professor Oscar Zariski on the occasion of his sixtieth birthday.

1. Introduction. The theorem of completeness of characteristic systems of complete continuous systems of curves on algebraic surfaces, conceived by Italian geometers around 1900 (see [8], no. 4, pp. 39-42), was first proved in 1921 by Severi [6] under the assumption that the curves are arithmetically effective. His proof is based on a theorem of fundamental importance due to Poincaré [9], [10] (see also Zariski [12]). Later, Severi [7] removed the assumption of arithmetical effectiveness and proved the theorem of completeness for semi-regular curves. We remark that a curve C on a surface is called semi-regular by Severi if the canonical linear system of the surface cuts out on C a complete linear system. In Section 2, we formulate this concept of semi-regularity in terms of sheaves in a form which is applicable to submanifolds of co-dimension 1 of higher dimensional complex manifolds.

A theorem of completeness of characteristic systems of complete continuous systems of submanifolds of co-dimension 1 on higher dimensional algebraic manifolds was proved by Kodaira [2], [3], under the assumption that the systems are "ample" in a certain sense. However, his proof, based essentially on the theory of harmonic differential forms, is indirect and does not reveal the real nature of the theorem. Moreover, his theorem does not cover Severi's result mentioned above since his "ampleness" is stronger than Severi's semi-regularity.

The purpose of this note is to prove, by an elementary direct method, the theorem of completeness of characteristic systems of complete continuous

* Received September 15, 1958.

[1] The first named author was supported during a portion of the period of preparation of this paper by the National Science Foundation (Research Grant G3248, Institute for Advanced Study); both authors were supported during the final phases of the preparation of the paper by the Office of Ordnance Research, U. S. Army (Contract DA-36-034-ORD-2164, Princeton University).

systems for semi-regular submanifolds of co-dimension 1 of higher dimensional manifolds. Our result covers as special cases both the theorem of Severi and that of Kodaira, and it holds also for an arbitrary non-algebraic complex manifold which need not even be compact. Moreover, our direct method of proof based on the theory of sheaves is quite elementary and involves only local considerations confined to a neighborhood of a given submanifold. The argument shows clearly that semi-regularity is just the right condition for the theorem of completeness. We remark finally that it seems impossible to find any *useful* necessary and sufficient condition for the theorem of completeness.

2. Formulation of the theorem. By a complex analytic fibre space we mean a triple $(\mathcal{V}, \varpi, M)$ of connected complex manifolds $\mathcal{V}$, M and a holomorphic map ϖ of $\mathcal{V}$ onto M. A fibre $V_t = \varpi^{-1}(t)$, $t \in M$, of the complex analytic fibre space will be called singular if there exists a point $p \in V_t$ such that the rank of the Jacobian of the map ϖ at p is less than the (complex) dimension of M. A complex analytic family of compact, complex manifolds is, by definition, a complex analytic fibre space without singular fibres whose fibres are compact and connected (see Kodaira and Spencer [4], §1). Now let W be a paracompact (but not necessarily compact) complex manifold. *By a complex analytic family of compact submanifolds of W we mean a complex analytic family $\mathcal{V} \xrightarrow{\varpi} M$ of compact complex manifolds such that each fibre $V_t = \varpi^{-1}(t)$ is a complex submanifold of W together with a holomorphic map Φ of $\mathcal{V}$ into W whose restriction to each fibre V_t is the inclusion map $V_t \to W$* (see Kodaira and Spencer [4], §12).[2] Denote a point on $\mathcal{V}$ by p. Clearly $p \to (\Phi(p), \varpi(p))$ is a biregular map of $\mathcal{V}$ into $W \times M$. We identify p with $(\Phi(p), \varpi(p)) \in W \times M$ and consider $\mathcal{V}$ as a *submanifold* of $W \times M$. Let $\pi : W \times M \to M$ be the canonical projection of $W \times M$ onto M. Then ϖ coincides with the restriction of π to $\mathcal{V}$: $\varpi = \pi \mid \mathcal{V}$. Conversely, *we may define a complex analytic family of compact submanifolds of W as a submanifold $\mathcal{V}$ of $W \times M$ such that $(\mathcal{V}, \pi \mid \mathcal{V}, M)$ forms a complex analytic family of compact complex manifolds* (see Weil [11], p. 881). In fact, the canonical projection $W \times M \to W$ induces a holomorphic map Φ of $\mathcal{V}$ into W, whose restriction to each fibre $V_t = \mathcal{V} \cap \pi^{-1}(t)$ is an inclusion map $V_t \to W$. In this note, we are exclusively concerned with complex analytic families of submanifolds of W of co-dimension 1.

Let $\mathcal{V} \xrightarrow{\varpi} M$ be a complex analytic family of compact submanifolds

[2] It is assumed in [4] that W is compact, but compactness of W is not required in the argument used here.

of a paracompact complex manifold W of co-dimension 1. We denote the (complex) dimension of the fibres $V_t = \varpi^{-1}(t)$ of $\mathfrak{V}$ by n; the dimension of W is therefore $n+1$. We may suppose that $\mathfrak{V} \subset W \times M$ and that $\varpi = \pi \mid \mathfrak{V}$, as was mentioned above. Clearly, $\mathfrak{V}$ is a submanifold of $W \times M$ of co-dimension 1, i.e., a *divisor* on $W \times M$. The divisor $\mathfrak{V}$ determines a complex line bundle $F = [\mathfrak{V}]$ over $W \times M$ (see for example Kodaira [3], p. 718). The restriction $F_t = F \mid W \times t$ of F to $\pi^{-1}(t) = W \times t$ may be considered as a complex line bundle over W by an obvious identification of $W \times t$ with W. We have $F_t = [V_t]$, since $V_t \times t$ is the divisor on $W \times t$ cut out by $\mathfrak{V}$. We denote by $\Omega(F_t)$ the sheaf over W of holomorphic sections of F_t and by Ψ_t the restriction of $\Omega(F_t)$ to V_t.

We denote by w a point on W and by $(w^1, w^2, \cdots, w^{n+1})$ the local holomorphic coordinates (not specified) of w. Consider a small "spherical" neighborhood N of a point on M and let $\{U_i\}$ be a locally finite covering of W by sufficiently small coordinate neighborhoods U_i. The submanifold $\mathfrak{V}$ of $W \times M$ is defined in each neighborhood $U_i \times N$ by a holomorphic equation

$$S_i(w, t) = 0, \tag{1}$$

where $S_i(w, t)$ is a holomorphic function on $U_i \times N$ such that

$$\sum_{\alpha=1}^{n+1} | \partial S_i(w, t)/\partial w^\alpha |^2 \neq 0$$

at each point (w, t) of $\mathfrak{V} \cap U_i \times N$ (if $\mathfrak{V} \cap U_i \times N$ is empty, we set $S_i(w, t) = 1$). Letting

$$S_i(w, t) = f_{ik}(w, t) S_k(w, t), \qquad w \in U_i \cap U_k, \tag{2}$$

we obtain a system $\{f_{ik}(w, t)\}$ of non-vanishing holomorphic functions $f_{ik}(w, t)$ defined, respectively, on $U_i \times N \cap U_k \times N$ satisfying

$$f_{ik}(w, t) = f_{ij}(w, t) f_{jk}(w, t), \qquad \text{for } w \in U_i \cap U_j \cap U_k. \tag{3}$$

Clearly, $\{f_{ik}(w, t)\}$ defines the complex line bundle $F \mid W \times N$ (the restriction of F to $W \times N$). Moreover, for each point $t \in N$, the submanifold V_t of W is defined in U_i by the holomorphic equation $S_i(w, t) = 0$ and the complex line bundle $F_t = [V_t]$ is defined by $\{f_{ik}(w, t)\}$.

Denote by $(t_1, \cdots, t_r, \cdots, t_m)$ a system of holomorphic coordinates on N. For any tangent vector

$$v = \sum_{r=1}^{m} v_r (\partial/\partial t_r)$$

of M at $t \in N$, we set

$$\psi_i(w,v) = -vS_i(w,t), \qquad \text{for } w \in V_t \cap U_i, \tag{4}$$

where

$$vS_i(w,t) = \sum_{r=1}^{m} v_r \partial S_i(w,t)/\partial t_r.$$

Since $S_i(w,t) = 0$ for $w \in V_t$, it follows from (2) that

$$\psi_i(w,v) = f_{ik}(w,t)\psi_k(w,v) \qquad \text{for } w \in V_t \cap U_i \cap U_k. \tag{5}$$

This shows that

$$\psi(v) : w \to (w, \psi_i(w,v))$$

is a holomorphic section of F_t over V_t. Thus, for each tangent vector v of M at t, we obtain an element $\psi(v)$ of $H^0(V_t, \Psi_t)$. We call $\psi(v) \in H^0(V_t, \Psi_t)$ *the infinitesimal displacement of* V along v and denote it by $\rho_{d,t}(v)$ (see Kodaira and Spencer [4], § 12). Denote by T_t the tangent space of M at t. It is clear that

$$\rho_{d,t} : v \to \rho_{d,t}(v) = \psi(v) \tag{6}$$

is a linear map of T_t into $H^0(V_t, \Psi_t)$.

For any element ψ of $H^0(V_t, \Psi_t)$ we denote by (ψ) the divisor of ψ. The set of all divisors (ψ), $\psi \in H^0(V_t, \Psi_t)$, forms a complete linear system L_t on V_t (see Kodaira [3], p. 718). The *characteristic system* of the family $\mathcal{V} \xrightarrow{\varpi} M$ on V_t is, by definition, the linear subsystem of L_t consisting of the divisors $(\rho_{d,t}(v))$ of infinitesimal displacements $\rho_{d,t}(v)$, $v \in T_t$ (see Kodaira [3], p. 738), and is said to be *complete* if and only if it coincides with the complete linear system L_t. In view of the one-to-one correspondonce between linear subsystems of L_t and linear subspaces of $H^0(V_t, \Psi_t)$, *the characteristic system of* $\mathcal{V} \xrightarrow{\varpi} M$ *on* V_t *is complete if and only if the map* $\rho_{d,t} : T_t \to H^1(V_t, \Psi_t)$ *is surjective.*

Let $\mathcal{V} \xrightarrow{\varpi} M$ be a complex analytic family of compact submanifolds of W and let t_0 be a point on M. We say that $\mathcal{V} \xrightarrow{\varpi} M$ is *maximal* at t_0 if, for any complex analytic family $\mathcal{V}' \xrightarrow{\varpi'} M'$ of compact submanifolds of W such that $\varpi^{-1}(t_0) = \varpi'^{-1}(t'_0)$, $t'_0 \in M'$, there exists a holomorphic map h of a neighborhood N' of t'_0 on M' into M which maps t'_0 into t_0 such that $\varpi'^{-1}(t') = \varpi^{-1}(h(t'))$ for $t' \in N'$, where we indicate by $\varpi'^{-1}(t') = \varpi^{-1}(t)$ that $\varpi'^{-1}(t')$ and $\varpi^{-1}(t)$ are the *same* submanifold of W. We note that, if $\varpi'^{-1}(t') = \varpi^{-1}(h(t'))$ for $t' \in N'$, there exists a holomorphic map h_* of $\mathcal{V}' \mid N' = \varpi'^{-1}(N')$ into $\mathcal{V}$ which maps each fibre $\varpi'^{-1}(t')$ biregularly onto $\varpi^{-1}(h(t'))$ and therefore $\mathcal{V}' \mid N'$ is the family induced from $\mathcal{V}$ by the map h. In fact, if we denote by $\hat{h}$ the holomorphic map: $(w,t') \to (w, h(t'))$ of

$W \times N'$ into $W \times M$ and if we suppose that $\mathfrak{V}' \mid N' \subset W \times N'$, $\mathfrak{V} \subset W \times M$, the restriction of $\hat{h}$ to $\mathfrak{V}' \mid N'$ gives h_*. Thus, if $\mathfrak{V} \xrightarrow{\varpi} M$ is maximal at t_0, $\mathfrak{V} \xrightarrow{\varpi} M$ is complete relative to W at t_0 (see Kodaira and Spencer [4], § 12).

Now we formulate our main theorem. In what follows we denote by M a spherical domain:

$$M = \{t \mid t = (t_1, t_2, \cdots, t_m), \qquad |t_1|^2 + \cdots + |t^2_m| < \delta\},$$

where $\delta > 0$. Let V_0 be a compact submanifold of W of co-dimension 1 and let $F_0 = [V_0]$ be the complex line bundle over W determined by V_0. Moreover, let $\Omega(F_0)$ be the sheaf over W of holomorphic sections of F_0 and let Ψ_0 be the restriction of $\Omega(F_0)$ to V_0. We denote by r_0 the restriction map: $\Omega(F_0) \to \Psi_0$. r_0 induces a homomorphism $r_0^*\colon H^1(W, \Omega(F_0)) \to H^1(V_0, \Psi_0)$ in a canonical manner.

DEFINITION. *We say that V_0 is semi-regular if the image*

$$r_0^* H^1(W, \Omega(F_0))$$

is zero.

In case W is an algebraic surface, our definition of semi-regularity is equivalent to Severi's definition mentioned in Section 1. To show this, let K be the canonical bundle on W and let $K_0 = K \mid V_0$ be the restriction of K to V_0. We remark that the canonical system $|K|$ cuts out on V_0 a complete linear system if and only if the restriction map

$$r_0\colon H^0(W, \Omega(K)) \to H^0(V_0, \Omega(K_0))$$

is surjective. Consider the exact sequence

$$0 \to \Omega \to \Omega(F_0) \xrightarrow{r_0} \Psi_0 \to 0,$$

where Ω denotes the sheaf over W of germs of holomorphic functions. By the duality theorem, the corresponding exact cohomology sequence

$$\cdots \to H^1(W, \Omega(F_0)) \xrightarrow{r_0^*} H^1(V_0, \Psi_0) \to H^2(W, \Omega) \to \cdots$$

is *dual* to

$$\cdots \leftarrow H^1(W, \Omega(K \otimes F_0^{-1})) \leftarrow H^0(V_0, \Omega(K_0)) \xleftarrow{r_0} H^0(W, \Omega(K)) \leftarrow \cdots.$$

It follows that the image $r_0^* H^1(W, \Omega(F_0))$ is zero if and only if r_0: $H^0(W, \Omega(K)) \to H^0(V_0, \Omega(K_0))$ is surjective.

MAIN THEOREM. *If a compact submanifold V_0 of W of codimension* 1 *is semi-regular, then there exists a complex analytic family* $\mathcal{V} \xrightarrow{\varpi} M$ *of compact submanifolds of W containing V_0 as the fibre $\varpi^{-1}(0)$ over $0 \in M$ such that, for each point $t \in M$, $\rho_{d,t}$ maps the tangent space T_t of M at t isomorphically onto $H^0(V_t, \Psi_t)$, where $V_t = \varpi^{-1}(t)$. Moreover, the family* $\mathcal{V} \xrightarrow{\varpi} M$ *is maximal at each point t of M.*

Now we apply our main theorem to the case in which W is an algebraic manifold imbedded in a projective space. Let V_0 be a submanifold of W of codimension 1. It is well known that the set $\mathcal{S}$ of all effective divisors $X \approx V_0$ on W, where $\approx$ denotes homology with integer coefficients, forms an algebraic system, i. e., there exist a (possibly reducible and singular) algebraic variety Σ and a one-to-one algebraic correspondence $\sigma \rightarrow X = X_\sigma$ between Σ and $\mathcal{S}$ (see Weil [11], p. 887). Σ is called the parameter variety of $\mathcal{S}$. The parameter variety Σ may be determined in the following manner (see Weil [11], p. 887; cf. also Kodaira [3], pp. 734-735). Take a hypersurface section E of W of sufficiently high order and consider the algebraic system $\mathcal{B}$ of all effective divisors $D \approx V_0 + E$ on W. The parameter variety Λ of $\mathcal{B}$ is a non-singular algebraic variety imbedded in a projective space. Let $\lambda \rightarrow D_\lambda$ be the one-to-one algebraic corerspondence between Λ and $\mathcal{B}$. Moreover, denote by $D_\lambda > E$ that $D_\lambda - E$ is effective. Then Σ is the subvariety of Λ consisting of all points λ such that $D_\lambda > E$ and, for each point $\sigma \in \Sigma \subset \Lambda$, the corresponding divisor $X_\sigma \in \mathcal{S}$ is given by $X_\sigma = D_\sigma - E$. We call the parameter variety Σ thus determined the *canonical parameter variety* of $\mathcal{S}$.

Suppose that V_0 is semi-regular and let $\mathcal{V} \xrightarrow{\varpi} M$ be the complex analytic family given in our main theorem. It follows from the bijectivity of $\rho_{d,t}$ that $V_t \neq V_s$ for $t \neq s$, provided that t and s are contained in a small neighborhood of a point on M. Hence, replacing M by a smaller spherical subdomain, if necessary, we may assume that $V_t \neq V_s$ for $t \neq s$, $t \in M$, $s \in M$. Since $V_t \approx V_0$, there exists for each $t \in M$ a point $\lambda(t) \in \Sigma \subset \Lambda$ such that $V_t = X_{\lambda(t)}$. By a result of Weil [11], the map $t \rightarrow \lambda(t)$ thus defined is *analytic* in the sense that the graph of the map $t \rightarrow \lambda(t)$ is an analytic subvariety of $M \times \Lambda$, while $t \rightarrow \lambda(t)$ is obviously one-to-one and continuous. It follows that $t \rightarrow \lambda(t)$ is regular analytic. Moreover, we infer from the bijectivity of $\rho_{d,t}$ that $t \rightarrow \lambda(t)$ *is biregular.* In fact, let N be a small neighborhood of a point t_0 on M and let $\{U_i\}$ be a finite covering of W. Moreover, let $S_i(w, t)$ be the holomorphic functions which defines $\mathcal{V}$ on $U_i \times N$ (see (1)). Let B be a neighborhood of $\lambda(t_0)$ on Λ. For $\lambda \in B$ the divisor D_λ is defined in each U_i by

$$R_i(w, \lambda) = 0,$$

where $R_i(w, \lambda)$ is a holomorphic function of w and λ. It follows from $D_{\lambda(t)} = V_t + E$ that

$$f_i(w, t) = R_i(w, \lambda(t))/S_i(w, t)$$

is a holomorphic function in w and t and that $f_i(w, t)$ does not vanish if $E \cap U_i$ is empty. Applying $\partial/\partial t_r$, we obtain from

$$f_i(w, t) S_i(w, t) = R_i(w, \lambda(t))$$

the equality

$$(7) \qquad f_i(w, t) \psi_i(w, \partial/\partial t_r) = -\sum_\nu (\partial\lambda_\nu(t)/\partial t_r) \cdot (\partial R_i(w, \lambda(t))/\partial\lambda_\nu) \quad \text{for } w \in V_t \cap U_i,$$

where $(\lambda_1, \cdots, \lambda_\nu, \cdots)$ denotes the local coordinates of λ. The bijectivity of $\rho_{d,t}$ implies that $\psi(\partial/\partial t_r) = \rho_{d,t}(\partial/\partial t_r)$, $r = 1, 2, \cdots, m$, are linearly independent. Therefore, considering U_i such that $E \cap U_i$ is empty, we infer from (7) that the rank of the Jacobian

$$\partial(\lambda_1, \lambda_2, \cdots, \lambda_\nu, \cdots)/\partial(t_1, t_2, \cdots, t_m)$$

of the map $t \to \lambda(t)$ is equal to m. This proves that $t \to \lambda(t)$ is biregular.

Now, since $\mathcal{V} \xrightarrow{\varpi} M$ is maximal at each point $t \in M$, we infer that the image $\lambda(M) \subset \Sigma$ is an *open* subset of Σ. Thus the point $\lambda(0)$ has the neighborhood $\lambda(M)$ on Σ which is analytically homeomorphic to the spherical domain M and hence $\lambda(0)$ is a simple point of Σ. Moreover the restriction $\mathcal{S} \mid \lambda(M) = \{X_\sigma \mid \sigma \in \lambda(M)\}$ of the algebraic system $\mathcal{S}$ to $\lambda(M)$ is a complex analytic family which is complex analytically eqivalent to $\mathcal{V} \to M$. Hence the characteristic system of $\mathcal{S}$ on $X_{\lambda(0)} = V_0$ can be defined and coincides with the characteristic system of $\mathcal{V}$ on V_0. It is therefore complete.

A *continuous system* is, by definition, an algebraic system whose parameter variety is irreducible. A continuous system is called *complete* if it is maximal in the sense that it is not contained in a larger continuous system. The parameter variety $\Sigma \subset \Lambda$ is composed of a finite number of irreducible components:

$$\Sigma = \Sigma' \cup \Sigma'' \cup \cdots \cup \Sigma^{(l)} \cup \cdots.$$

Corresponding to this, $\mathcal{S}$ is composed of a finite number of complete continuous systems $\mathcal{S}', \mathcal{S}'', \cdots, \mathcal{S}^{(l)}, \cdots$, where $\mathcal{S}^{(l)} = \mathcal{S} \mid \Sigma^{(l)} = \{X_\sigma \mid \sigma \in \Sigma^{(l)}\}$. It is clear that the simple point $\lambda(0)$ of Σ belongs to one and only one irreducible component, say Σ'. Hence $V_0 = X_{\lambda(0)}$ belongs to one and only one complete continuous system $\mathcal{S}'$. Thus we obtain

THEOREM (*Completeness of characteristic systems*). *Let W be an algebraic manifold imbedded in a projective space and let V_0 be a submanifold of W of codimension* 1. *If V_0 is semi-regular, then V_0 belongs to only one complete continuous system $\mathcal{S}'$ of effective divisors on W and V_0 corresponds to a simple point of the canonical parameter variety Σ' of $\mathcal{S}'$. Moreover, the characteristic system of $\mathcal{S}'$ on V_0 is complete.*

This theorem covers as special cases both the theorem of Severi [7] and that of Kodaira [3].

3. Construction of a complex analytic family. Let W be a paracompact complex manifold of complex dimension $n+1 \geqq 2$ and let V_0 be a compact submanifold of W of dimension n. In what follows we denote by p a point on W and by $(w^1(p), w^2(p), \cdots, w^{n+1}(p))$ the coordinate of p with respect to a system of local holomorphic coordinates $(w^1, w^2, \cdots, w^{n+1})$ on W. We choose a locally finite covering $\mathfrak{U} = \{U_i\}$ of W such that i) each neighborhood U_i is a polycylinder:

$$U_i = \{p \mid |w^1{}_i(p)| < 1, |w^2{}_i(p)| < 1, \cdots, |w^{n+1}{}_i(p)| < 1\},$$

where $(w^1{}_i, w^2{}_i, \cdots, w^{n+1}{}_i)$ is a system of local holomorphic coordinates which covers the closure of U_i (thus the closure of U_i is compact), ii) $V_0 \cap U_i$ coincides with the coordinate plane $w^{n+1}{}_i = 0$ if $V_0 \cap U_i$ is not empty, and such that iii) $V_0 \cap U_i \cap U_k$ is not empty if $V_0 \cap U_i$, $V_0 \cap U_k$ and $U_i \cap U_k$ are not empty. Moreover, if $V_0 \cap U_i$ is not empty, we write for convenience

$$w_i = w^{n+1}{}_i,\ z^1{}_i = w^1{}_i, \cdots, z^n{}_i = w^n{}_i.$$

Let

$$S_{i|0}(p) = \begin{cases} w_i(p), & \text{if } V_0 \cap U_i \neq \text{empty}, \\ 1\ , & \text{if } V_0 \cap U_i = \text{empty}, \end{cases}$$

and let

$$f_{ik|0}(p) = S_{i|0}(p)/S_{k|0}(p), \qquad \text{for } p \in U_i \cap U_k. \tag{8}$$

Clearly, $f_{ik|0}(p)$ are non-vanishing holomorphic functions defined on $U_i \cap U_k$, respectively, and the system $\{f_{ik|0}(p)\}$ defines the complex line bundle $F_0 = [V_0]$. More precisely, we have the product representation

$$F_0 \mid U_i = U_i \times \boldsymbol{C} \tag{9}$$

of each piece $F_0 \mid U_i$, where $(p, \zeta_i) \in U_i \times \boldsymbol{C}$ is identical with $(p, \zeta_k) \in U_k \times \boldsymbol{C}$ if and only if $\zeta_i = f_{ik|0}(p)\zeta_k$. Let Ψ_0 be the restriction of $\Omega(F_0)$ to V_0 and let $\{\beta_1, \cdots, \beta_r, \cdots, \beta_m\}$ be a base of the linear space $H^0(V_0, \Psi_0)$. Each

β_r is a holomorphic section of F_0 over V_0 and therefore β_r is written in the form

$$\beta_r\colon p \to (p, \beta_{ri}(p))$$

with respect to the product representation (9), where $\beta_{ri}(p)$ are holomorphic functions on $V_0 \cap U_i$ satisfying

$$\beta_{ri}(p) = f_{ik|0}(p)\beta_{rk}(p), \qquad \text{for } p \in V_0 \cap U_i \cap U_k. \tag{10}$$

First we prove the following

THEOREM 1. *If V_0 is semi-regular, then there exists a complex analytic family $\mathcal{V} \xrightarrow{\varpi} M$ of compact submanifolds of W containing V_0 as the fibre $\varpi^{-1}(0)$ over $0 \in M$ such that $\rho_{d,0}$ maps the tangent space T_0 of M at 0 isomorphically onto $H^0(V_0, \Psi_0)$.*

Let N be a spherical neighborhood of 0 on the space of m complex variables $t_1, t_2, \cdots, t_m$, where $m = \dim H^0(V_0, \Psi_0)$. In order to prove the above Theorem 1, is suffices to construct a system $\{S_i(p,t)\}$ of holomorphic functions $S_i(p,t)$ defined respectively on $U_i \times N$ and a system $\{f_{ik}(p,t)\}$ of non-vanishing holomorphic functions $f_{ik}(p,t)$ defined respectively on $U_i \cap U_k \times N$ such that

$$S_i(p,t) = f_{ik}(p,t)S_k(p,t), \qquad \text{for } p \in U_i \cap U_k, \tag{11}$$

$$S_i(p,0) = S_{i|0}(p), \qquad f_{ik}(p,0) = f_{ik|0}(p), \tag{12}$$

$$S_i(p,t) \neq 0, \qquad \text{if } V_0 \cap U_i = \text{empty}, \tag{12a}$$

$$\partial S_i(p,t)/\partial t_r \,|_{t=0} = \beta_{ri}(p). \tag{13}$$

In fact, letting $M \subset N$ be a sufficiently small spherical subdomain with the center 0, $\mathcal{V} \to M$ is given as the submanifold $\mathcal{V} \subset W \times M$ defined by the holomorphic equations $S_i(p,t) = 0$.

We write $S_i(p,t)$, $f_{ik}(p,t)$ in the forms

$$S_i(p,t) = S_{i|0}(p) + \sum_{\mu=1}^{\infty} S_{i|\mu}(p,t),$$

$$f_{ik}(p,t) = f_{ik|0}(p) + \sum_{\mu=1}^{\infty} f_{ik|\mu}(p,t),$$

where $S_{i|\mu}(p,t)$, $f_{ik|\mu}(p,t)$ are homogeneous polynomials in $t = (t_1, t_2, \cdots, t_m)$ of degree μ whose coefficients are holomorphic functions on U_i, $U_i \cap U_k$, respectively. Let

$$S^{\mu}{}_i(p,t) = S_{i|0}(p) + \sum_{\lambda=1}^{\mu} S_{i|\lambda}(p,t), \tag{14}$$

$$f^{\mu}_{ik}(p,t)=f_{ik|0}(p)+\sum_{\lambda=1}^{\mu} f_{ik|\lambda}(p,t). \tag{15}$$

Moreover, for arbitrary power series $P(t)$, $Q(t)$, in t, we indicate by $P(t)\underset{\mu}{\equiv}Q(t)$ that $P(t)-Q(t)$ contains no terms of degree $\leqq\mu$ in t. Clearly, the equality (11) is equivalent to the system of congruences

$$S^{\mu}_{i}(p,t)\underset{\mu}{\equiv}f^{\mu}_{ik}(p,t)S^{\mu}_{k}(p,t), \qquad \mu=1,2,3,\cdots. \tag*{$(16)_\mu$}$$

In order to construct $S_{i|\mu}(p,t)$, $f_{ik|\mu}(p,t)$ by induction on μ, we assume the following special forms for $S_{i|\mu}(p,t)$, $\mu\geqq 1$:

$$S_{i|\mu}(p,t)=\begin{cases}\psi_{i|\mu}(z_i(p),t), & \text{if } V_0\cap U_i\neq\text{empty},\\ 0\quad , & \text{if } V_0\cap U_i=\text{empty},\end{cases} \tag{17}$$

where $z_i(p)=(z^1_i(p),\cdots,z^n_i(p))$ and $\psi_{i|\mu}(z_i,t)$ is a homogeneous polynomial of degree μ in t whose coefficients are holomorphic functions of $z_i=(z^1_i,\cdots,z^n_i)$ defined on the polycylinder: $|z^1_i|<1,\cdots,|z^n_i|<1$.

First, we define $\psi_{i|1}(z_i,t)$ by

$$\psi_{i|1}(z_i(p),t)=\sum_{r=1}^{m} t_r\beta_{ri}(p), \qquad \text{for } p\in V_0\cap U_i, \tag{18}$$

and determine $S_{i|1}(p,t)$, $S^1_i(p,t)$ by (17), (14). The congruence $(16)_1$ is equivalent to

$$S_{i|1}(p,t)=f_{ik|0}(p)S_{k|1}(p,t)+f_{ik|1}(p,t)S_{k|0}(p).$$

Hence, letting

$$f_{ik|1}(p,t)=\{S_{i|1}(p,t)-f_{ik|0}(p)S_{k|1}(p,t)\}/S_{k|0}(p),$$

we obtain $f^1_{ik}(p,t)=f_{ik|0}(p)+f_{ik|1}(p,t)$ satisfying $(16)_1$, provided that $f_{ik|1}(p,t)$ is holomorphic in p. Now it follows from (10) and (18) that

$$S_{i|1}(p,t)-f_{ik|0}(p)S_{k|1}(p,t)=0 \qquad \text{for } p\in V_0\cap U_i\cap U_k.$$

We infer therefore that $f_{ik|1}(p,t)$ is holomorphic in p.

Now suppose that $S^{\mu}_i(p,t)$, $f^{\mu}_{ik}(p,t)$ satisfying $(16)_\mu$ are already determined. Clearly, $(16)_\mu$ implies that

$$f^{\mu}_{ik}(p,t)\underset{\mu}{\equiv}f^{\mu}_{ij}(p,t)f^{\mu}_{jk}(p,t), \qquad p\in U_i\cap U_j\cap U_k. \tag*{$(19)_\mu$}$$

We define homogeneous polynomials $\psi_{ik|\mu+1}(p,t)$ in t of degree $\mu+1$ whose coefficients are holomorphic functions on $V_0\cap U_i\cap U_k$ by

$$\psi_{ik|\mu+1}(p,t)\underset{\mu+1}{\equiv}f^{\mu}_{ik}(p,t)S^{\mu}_k(p,t)-S^{\mu}_i(p,t) \qquad \text{for } p\in V_0\cap U_i\cap U_k.$$

Then we have

$$(20)\qquad \psi_{ik|\mu+1}(p,t)=\psi_{ij|\mu+1}(p,t)+f_{ij|0}(p)\psi_{jk|\mu+1}(p,t),\qquad \text{for } p\in V_0\cap U_i\cap U_j\cap U_k.$$

In fact, letting $\psi_{ik|\mu+1}=\psi_{ik|\mu+1}(p,t)$, $f^{\mu}{}_{ik}=f^{\mu}{}_{ik}(p,t)$, $S^{\mu}{}_i=S^{\mu}{}_i(p,t),\cdots,$ we have

$$\begin{aligned}\psi_{ij|\mu+1}+f_{ij|0}\psi_{jk|\mu+1} &\underset{\mu+1}{\equiv} f^{\mu}{}_{ij}S^{\mu}{}_j-S^{\mu}{}_i+f_{ij|0}f^{\mu}{}_{jk}S^{\mu}{}_k-f_{ij|0}S^{\mu}{}_j\\ &\underset{\mu+1}{\equiv}(f^{\mu}{}_{ij}-f_{ij|0})S^{\mu}{}_j+f_{ij|0}f^{\mu}{}_{jk}S^{\mu}{}_k-S^{\mu}{}_i\\ &\underset{\mu+1}{\equiv}(f^{\mu}{}_{ij}-f_{ij|0})f^{\mu}{}_{jk}S^{\mu}{}_k+f_{ij|0}f^{\mu}{}_{jk}S^{\mu}{}_k-S^{\mu}{}_i\\ &\underset{\mu+1}{\equiv} f^{\mu}{}_{ij}f^{\mu}{}_{jk}S^{\mu}{}_k-S^{\mu}{}_i,\end{aligned}$$

while

$$S^{\mu}{}_k(p,t)=\sum_{\lambda=1}^{\mu}\psi_{k|\lambda}(z_k(p),t)\underset{0}{\equiv}0\qquad \text{for } p\in V_0\cap V_k.$$

Hence by $(19)_{\mu}$, we obtain, for $p\in V_0\cap U_i\cap U_k\cap U_j$,

$$\psi_{ij|\mu+1}+f_{ij|0}\psi_{jk|\mu+1}\underset{\mu+1}{\equiv} f^{\mu}{}_{ik}S^{\mu}{}_k-S^{\mu}{}_i\underset{\mu+1}{\equiv}\psi_{ik|\mu+1}.$$

This proves (20). (20) shows that the system $\{\psi_{ik|\mu+1}(p,t)\}$ is a homogeneous polynomial in t of order $\mu+1$, whose coefficients are 1-cocycles on the nerve of the covering $\mathfrak{U}\mid V_0=\{V_0\cap U_i\}$ of V_0 with coefficients in the sheaf Ψ_0. Since the polycylinders $V_0\cap U_i$ are Stein manifolds, we have the *canonical isomorphism*

$$H^1(\mathfrak{U}\mid V_0,\Psi_0)\cong H^1(V_0,\Psi_0)$$

(see Cartan [1], Leray [5]). The 1-cocycle $\{\psi_{ik|\mu+1}(p,t)\}$ represents a homogeneous polynomial $\psi_{\mu+1}(t)$ in t of degree $\mu+1$ with coefficients in $H^1(V_0,\Psi_0)$. We may call $\psi_{\mu+1}(t)$ the *μ-th obstruction.*

If the obstruction $\psi_{\mu+1}(t)$ vanishes identically, we can construct $S^{\mu+1}{}_i(p,t)$, $f^{\mu+1}{}_{ik}(p,t)$ satisfying $(16)_{\mu+1}$. In fact, in view of the canonical isomorphism mentioned above, the vanishing of $\psi_{\mu+1}(t)$ implies the existence of homogeneous polynomials $\phi_{i|\mu+1}(p,t)$ in t of degree $\mu+1$ whose coefficients are holomorphic functions on $V_0\cap U_i$ such that

$$(21)\qquad \psi_{ik|\mu+1}(p,t)=\phi_{i|\mu+1}(p,t)-f_{ik|0}(p)\phi_{k|\mu+1}(p,t),\qquad \text{for } p\in V_0\cap U_i\cap U_k.$$

We define $\psi_{i|\mu+1}(z_i,t)$ by

$$\psi_{i|\mu+1}(z_i(p),t)=\phi_{i|\mu+1}(p,t),\qquad \text{for } p\in U_0\cap U_i$$

and determine $S_{i|\mu+1}(p,t)$ by (17), $S^{\mu+1}{}_i(p,t)$ by (14). Then letting

$$\Xi^{(\mu)}{}_{ik}(p,t) = S^{\mu}{}_i(p,t) - f^{\mu}{}_{ik}(p,t)S^{\mu}{}_k(p,t) + S_{i|\mu+1}(p,t) - f_{ik|0}(p)S_{k|\mu+1}(p,t),$$

we define $f_{ik|\mu+1}(p,t)$ by

$$f_{ik|\mu+1}(p,t) \underset{\mu+1}{\equiv} \Xi^{(\mu)}{}_{ik}(p,t)/S_{k|0}(p)$$

and determine $f^{\mu+1}{}_{ik}(p,t)$ by (15). We infer from (21) that

$$\Xi^{(\mu)}{}_{ik}(p,t) \underset{\mu+1}{\equiv} 0 \qquad \text{for } p \in V_0 \cap U_i \cap U_k.$$

Hence $f_{ik|\mu+1}(p,t)$ are holomorphic in p. It is easy to verify that $S^{\mu+1}{}_i(p,t)$ and $f^{\mu+1}{}_{ik}(p,t)$ thus defined satisfy $(16)_{\mu+1}$.

Now we prove that *the obstruction $\psi_{\mu+1}(t)$ vanishes identically if V_0 is semi-regular.* For this purpose it suffices to construct a polynomial $\{\eta_{ik}(p,t)\}$ in t of degree $\mu+1$ whose coefficients form a 1-cocycle on the nerve of the covering $\mathfrak{U}=\{U_i\}$ of W with coefficients in $\Omega(F_0)$ such that

$$(22) \qquad \psi_{ik|\mu+1}(p,t) = \eta_{ik}(p,t) \qquad \text{for } p \in V_0 \cap U_i \cap U_k.$$

In fact, $\{\eta_{ik}(p,t)\}$ represents a polynomial $\eta(t)$ in t with coefficients in $H^1(W,\Omega(F_0))$ and (22) implies that $\psi_{\mu+1}(t) = r_0{}^*\eta(t)$. Hence we obtain $\psi_{\mu+1}(t)=0$ if V_0 is semi-regular.

LEMMA 1. *For each positive integer $\lambda \leqq \mu$, there exist polynomials $g^{\lambda}{}_{ik}(p,t)$ in t of degree λ whose coefficients are holomorphic functions in p defined on $U_i \cap U_k$ such that*

$$(23)_{\lambda} \qquad g^{\lambda}{}_{ik}(p,t) = g^{\lambda}{}_{ij}(p,t) + g^{\lambda}{}_{jk}(p,t) \qquad \text{for } p \in U_i \cap U_j \cap U_k,$$

$$(24)_{\lambda} \qquad f_{ik|0}(p) \exp g^{\lambda}{}_{ik}(p,t) \underset{\lambda}{\equiv} f^{\lambda}{}_{ik}(p,t).$$

Proof. By induction on $\lambda \leqq \mu$. Assume the existence of $g^{\lambda-1}{}_{ik} = g^{\lambda-1}{}_{ik}(p,t)$ satisfying $(23)_{\lambda-1}$ and $(24)_{\lambda-1}$. In view of $(24)_{\lambda-1}$ we can determine homogeneous polynomials $g_{ik|\lambda} = g_{ik|\lambda}(p,t)$ in t of degree λ whose coefficients are holomorphic functions on $U_i \cap U_k$ such that

$$f_{ik|0} \cdot (1 + g_{ik|\lambda}) \exp g^{\lambda-1}{}_{ik} \underset{\lambda}{\equiv} f^{\lambda}{}_{ik}.$$

The congruence $(19)_{\mu}$ implies that $f^{\lambda}{}_{ik} \underset{\lambda}{\equiv} f^{\lambda}{}_{ij} f^{\lambda}{}_{jk}$ for $\lambda \leqq \mu$. Hence we obtain

$$1 + g_{ik|\lambda} \underset{\lambda}{\equiv} (1 + g_{ij|\lambda})(1 + g_{jk|\lambda})$$

or

$$g_{ik|\lambda} = g_{ij|\lambda} + g_{jk|\lambda}.$$

Now let

$$g^{\lambda}{}_{ik}(p,t) = g^{\lambda-1}{}_{ik}(p,t) + g_{ik|\lambda}(p,t).$$

Clearly, $g^{\lambda}{}_{ik}(p,t)$ satisfy $(23)_\lambda$ and $(24)_\lambda$, q. e. d.

We define polynomials $\hat{f}^{\mu+1}{}_{ik} = \hat{f}^{\mu+1}{}_{ik}(p,t)$ in t of degree $\mu+1$ by

$$\hat{f}^{\mu+1}{}_{ik}(p,t) \underset{\mu+1}{\equiv} f_{ik|0}(p) \exp g^{\mu}{}_{ik}(p,t).$$

It follows from $(23)_\mu$ and $(24)_\mu$ that

$$\hat{f}^{\mu+1}{}_{ik} \underset{\mu+1}{\equiv} \hat{f}^{\mu+1}{}_{ij}\hat{f}^{\mu+1}{}_{jk}, \tag{25}$$

$$\hat{f}^{\mu+1}{}_{ik}(p,t) \underset{\mu}{\equiv} f^{\mu}{}_{ik}(p,t). \tag{26}$$

Combining (26) with $(16)_\mu$, we obtain

$$S^{\mu}{}_{i}(p,t) \underset{\mu}{\equiv} \hat{f}^{\mu+1}{}_{ik}(p,t) S^{\mu}{}_{k}(p,t). \tag{27}$$

In view of (27) we can determine homogeneous polynomials $\eta_{ik}(p,t)$ in t of degree $\mu+1$ whose coefficients are holomorphic functions on $U_i \cap U_k$ by

$$\eta_{ik}(p,t) \underset{\mu+1}{\equiv} \hat{f}^{\mu+1}{}_{ik}(p,t) S^{\mu}{}_{k}(p,t) - S^{\mu}{}_{i}(p,t).$$

We have

$$\eta_{ik}(p,t) = \eta_{ij}(p,t) + f_{ij|0}(p)\eta_{jk}(p,t).$$

In fact, using (27) and (25), we obtain

$$\begin{aligned}
\eta_{ij} + f_{ij|0}\eta_{jk} &\underset{\mu+1}{\equiv} \hat{f}^{\mu+1}{}_{ij}S^{\mu}{}_{j} - S^{\mu}{}_{i} + f_{ij|0}\hat{f}^{\mu+1}{}_{jk}S^{\mu}{}_{k} - f_{ij|0}S^{\mu}{}_{j} \\
&\underset{\mu+1}{\equiv} (\hat{f}^{\mu+1}{}_{ij} - f_{ij|0})S^{\mu}{}_{j} + f_{ij|0}\hat{f}^{\mu+1}{}_{jk}S^{\mu}{}_{k} - S^{\mu}{}_{i} \\
&\underset{\mu+1}{\equiv} (\hat{f}^{\mu+1}{}_{ij} - f_{ij|0})\hat{f}^{\mu+1}{}_{jk}S^{\mu}{}_{k} + f_{ij|0}\hat{f}^{\mu+1}{}_{jk}S^{\mu}{}_{k} - S^{\mu}{}_{i} \\
&\underset{\mu+1}{\equiv} \hat{f}^{\mu+1}{}_{ij}\hat{f}^{\mu+1}{}_{jk}S^{\mu}{}_{k} - S^{\mu}{}_{i} \underset{\mu+1}{\equiv} \hat{f}^{\mu+1}{}_{ik}S^{\mu}{}_{k} - S^{\mu}{}_{i} \underset{\mu+1}{\equiv} \eta_{ik}.
\end{aligned}$$

Thus $\{\eta_{ik}(p,t)\}$ is a polynomial in t whose coefficients are 1-cocycles on the nerve of $\mathfrak{U} = \{U_i\}$ with coefficients in $\Omega(F_0)$. Moreover, since $S^{\mu}{}_{k}(p,t) \underset{0}{\equiv} 0$ for $p \in V_0 \cap U_k$, we have

$$\eta_{ik}(p,t) \underset{\mu+1}{\equiv} f^{\mu}{}_{ik}(p,t) S^{\mu}{}_{k}(p,t) - S^{\mu}{}_{i}(p,t) \underset{\mu+1}{\equiv} \psi_{ik|\mu+1}(p,t)$$

for $p \in V_0 \cap U_i \cap U_k$. This proves (22).

Thus, in case V_0 is semi-regular, we can construct $S^{\mu}{}_{i}(p,t)$ and $\mathfrak{f}^{\mu}{}_{ik}(p,t)$ satisfying $(16)_\mu$ by induction on μ, and therefore we obtain $S_i(p,t)$ and $f_{ik}(p,t)$ satisfying (11), (12), (12a) and (13) which are *formal power series* in t.

4. Proof of convergence. Consider a formal power series

$$f(t) = f(p, t) = \sum f_{h_1 h_2 \cdots h_m}(p)\,(t_1)^{h_1}(t_2)^{h_2}\cdots(t_m)^{h_m}$$

whose coefficients $f_{h_1 h_2 \cdots h_m}(p)$ are holomorphic functions in p defined on a domain and a power series

$$a(t) = \sum a_{h_1 h_2 \cdots h_m}(t_1)^{h_1}(t_2)^{h_2}\cdots(t_m)^{h_m}, \qquad a_{h_1 h_2 \cdots h_m} \geqq 0.$$

We indicate by $f(p, t) \ll a(t)$ that

$$|f_{h_1 h_2 \cdots h_m}(p)| < a_{h_1 h_2 \cdots h_m};$$

moreover, we write $f(t) \ll a(t)$ if $f(p, t) \ll a(t)$ for each point p in the domain.

Let

$$A(t) = (b/64c) \sum_{\mu=1}^{\infty} c^{\mu}(t_1 + t_2 + \cdots + t_m)^{\mu}/\mu^2,$$

where b and c are positive constants. By a simple computation we obtain

$$A(t)^2 \ll (b/c) A(t). \tag{28}$$

In what follows we denote by $c_1, c_2, \cdots$ positive constants. Our purpose is to show that the above construction of the formal power series $S_i(p, t)$ and $f_{ik}(p, t)$ can be carried out in such a way that

$$S_i(t) - S_{i|0} \ll A(t),$$

$$f_{ik}(t) - f_{ik|0} \ll c_1 A(t),$$

provided that we choose the constants b, c, c_1 properly.

We may assume that

$$|f_{ik|0}(p)| < c_2, \qquad \text{for } p \in U_i \cap U_k. \tag{29}$$

It follows from (10) that the $\beta_{ri}(p)$ are bounded and therefore

$$S^1{}_i(t) - S_{i|0} \ll A(t), \tag{30}$$

provided that b is sufficiently large. Now, supposing that

$$f^{\mu-1}{}_{ik}(t) - f_{ik|0} \ll c_1 A(t), \tag{31}$$

$$S^{\mu}{}_i(t) - S_{i|0} \ll A(t), \tag{32}$$

we first prove

$$f^{\mu}{}_{ik}(t) - f_{ik|0} \ll c_1 A(t) \tag{33}$$

and then we show that $\phi_{i|\mu+1}(p,t)$ in (21) can be chosen in such a way that

$$(34)\qquad S^{\mu+1}{}_i - S_{i|0} \ll A(t).$$

It follows from $(16)_\mu$ that

$$(35)\qquad f_{ik|\mu}(p,t) \underset{\mu}{\equiv} \{S^\mu{}_i(p,t) - f^{\mu-1}{}_{ik}(p,t)S^\mu{}_k(p,t)\}/S_{k|0}(p).$$

We have

$$S^\mu{}_i - f^{\mu-1}{}_{ik}S^\mu{}_k = S^\mu{}_i - S_{i|0} - (f^{\mu-1}{}_{ik} - f_{ik|0})(S^\mu{}_k - S_{k|0})$$
$$- f_{ik|0}(S^\mu{}_k - S_{k|0}) - S_{k|0}(f^{\mu-1}{}_{ik} - f_{ik|0}),$$

while $S^\mu{}_i - f^{\mu-1}{}_{ik}S^\mu{}_k \underset{\mu-1}{\equiv} 0$, and therefore the term $S_{k|0}(f^{\mu-1}{}_{ik} - f_{ik|0})$ contributes nothing to $S^\mu{}_i - f^{\mu-1}{}_{ik}S^\mu{}_k$. Hence, using (31), (32), (29) and (28), we obtain

$$(36)\qquad S^\mu{}_i(t) - f^{\mu-1}{}_{ik}(t)S^\mu{}_k(t) \ll A(t) + c_1A(t)^2 + c_2A(t) \ll c_3A(t),$$

where

$$c_3 = 1 + (bc_1/c) + c_2.$$

Consider the case in which $U_k \cap V_0$ is *not* empty. Let $\{U^*{}_i\}$ be a covering of W such that *the closure of each $U^*{}_i$ is contained in U_i.* It is clear that, *if $p \in U^*{}_i \cap U_k$ and if $|w_k(p)| \leqq \epsilon$, the disk*

$$\Delta = \{q \mid z_k(q) = z_k(p), |w_k(q)| \leqq \epsilon\}$$

is contained in $U_i \cap U_k$, provided that the constant $\epsilon > 0$ is sufficiently small (we recall that $\{U_i\}$ is a locally finite covering and that $(z_k, w_k) = (z^1{}_k, \cdots, z^n{}_k, w_k)$ is a system of holomorphic coordinates which covers U_k and U_k is the polycylinder: $|z^1{}_k| < 1, \cdots, |z^n{}_k| < 1$, $|w_k| < 1$). We infer that

$$(37)\qquad f_{ik|\mu}(p,t) \ll (c_3/\epsilon)A(t), \qquad \text{for } p \in U^*{}_i \cap U_k.$$

In fact, in case $|w_k(p)| \geqq \epsilon$, (37) follows immediately from (35) and (36), since $S_{k|0}(p) = w_k(p)$. In case $|w_k(p)| < \epsilon$, we observe that each coefficient of $f_{ik|\mu}(t)$ is holomorphic on the disk $\Delta \subset U_i \cap U_k$ and that the estimate (37) is valid for each point on the periphery of Δ. Hence, by the maximum principle, (37) is valid for $p \in \Delta$. (37) is valid also in case $U_k \cap V_0$ is empty, provided that $\epsilon < 1$, since, in this case, $S_{k|0}(p) = 1$.

It follows from $f^\mu{}_{ik} \underset{\mu}{\equiv} f^\mu{}_{ij}f^\mu{}_{jk}$ that

$$(38)\qquad f_{ik|\mu} - f_{jk|0}f_{ij|\mu} - f_{ij|0}f_{jk|\mu} \underset{\mu}{\equiv} f^{\mu-1}{}_{ij}f^{\mu-1}{}_{jk} - f^{\mu-1}{}_{ik}.$$

We have

$$f^{\mu-1}_{ik}-f^{\mu-1}_{ij}f^{\mu-1}_{jk}=-(f^{\mu-1}_{ij}-f_{ij|0})(f^{\mu-1}_{jk}-f_{jk|0})$$
$$+f^{\mu-1}_{ik}-f_{jk|0}f^{\mu-1}_{ij}-f_{ij|0}f^{\mu-1}_{jk}+f_{ij|0},$$

while $f^{\mu-1}_{ik}-f^{\mu-1}_{ij}f^{\mu-1}_{jk}\underset{\mu-1}{\equiv}0$. Hence we infer from (31) that

$$f^{\mu-1}_{ik}(t)-f^{\mu-1}_{ij}(t)f^{\mu-1}_{jk}(t)\ll c_1^2A(t)^2\ll(bc_1^2/c)A(t)$$

and therefore, by (38),

$$f_{ik|\mu}(t)-f_{jk|0}f_{ij|\mu}(t)-f_{ij|0}f_{jk|\mu}(t)\ll(bc_1^2/c)A(t). \tag{39}$$

This implies that

$$f_{ji|0}f_{ij|\mu}(t)+f_{ij|0}f_{ji|\mu}(t)\ll(bc_1^2/c)A(t), \tag{40}$$

since $f_{ii|\mu}(t)=0$. Combining (37) and (40) and using (29), we get

$$f_{ik|\mu}(p,t)\ll((c_2^2c_3/\epsilon)+(bc_2c_1^2/c))A(t),\qquad \text{for } p\in U_i\cap U^*_k. \tag{41}$$

Now let p be any point of $U_i\cap U_k$. p is contained in one of the neighborhoods, say U^*_j. If $j=i$ or $j=k$, the estimate of $f_{ik|\mu}(p,t)$ is given already by (37) or (41). If $j\neq i$, $j\neq k$, the estimates of $f_{ij|\mu}(p,t)$ and $f_{jk|\mu}(p,t)$ are given by (41) and (37), respectively, and therefore, using (39), we cbtain

$$f_{ik|\mu}(p,t)\ll((c_2+c_2^3)(c_3/\epsilon)+(1+c_2^2)(bc_1^2/c))A(t).$$

We set

$$c_1=2\,(c_2+2)(c_2+c_2^3)/\epsilon$$

Clearly $c_2+2>c_3$ if $c>bc_1$. Consequently, if

$$c>2bc_1(1+c_2^2),$$

we get

$$(c_2+c_2^3)(c_3/\epsilon)+(1+c_2^2)(bc_1^2/c)<c_1$$

and therefore

$$f_{ik|\mu}(t)\ll c_1A(t).$$

Combined with (31), this proves (33).

Next, $\psi_{ik|\mu+1}(t)=\psi_{ik|\mu+1}(p,t)$ is defined by

$$\psi_{ik|\mu+1}(t)\underset{\mu+1}{\equiv}f^{\mu}_{ik}(t)S^{\mu}_k(t)-S^{\mu}_i(t).$$

We have

$$f^{\mu}_{ik}S^{\mu}_k-S^{\mu}_i=(f^{\mu}_{ik}-f_{ik|0})(S^{\mu}_k-S_{k|0})$$
$$+f_{ik|0}S^{\mu}_k+S_{k|0}f^{\mu}_{ik}-S^{\mu}_i-S_{i|0},$$

while $f^{\mu}_{ik}S^{\mu}_k-S^{\mu}_i\underset{\mu}{\equiv}0$. Hence it follows from (32) and (33) that

$$f^{\mu}_{ik}(t)S^{\mu}_{k}(t) - S^{\mu}_{i}(t) \ll c_1 A(t)^2 \ll (bc_1/c)A(t).$$

We obtain therefore

$$\psi_{ik|\mu+1}(t) \ll (bc_1/c)A(t). \tag{42}$$

LEMMA 2. *We can choose* $\phi_{i|\mu+1}(t) = \phi_{i|\mu+1}(p,t)$ *satisfying*

$$\phi_{i|\mu+1}(p,t) - f_{ik|0}(p)\phi_{k|\mu+1}(p,t) = \psi_{ik|\mu+1}(p,t)$$

such that

$$\phi_{i|\mu+1}(t) \ll (c_4 bc_1/c)A(t), \tag{43}$$

where the constant c_4 *is independent of* μ.

An elementary proof of this lemma will be given in Section 6 below.

Clearly (43) implies that

$$S_{i|\mu+1}(t) \ll (bc_1c_4/c)A(t).$$

Consequently, letting

$$c = 2bc_1(1 + c_2{}^2) + bc_1c_4,$$

we obtain (34).

Now, since the constants b, c, c_1 are independent of μ, we infer by induction on μ that

$$\begin{cases} f_{ik}(t) - f_{ik|0} \ll c_1 A(t), \\ S_i(t) - S_{i|0} \ll A(t). \end{cases} \tag{44}$$

Let $N = \{t \mid \sum_{r=1}^{m} |t_r|^2 < c^2/m\}$. It follows from (44) that the power series $S_i(p,t)$ and $f_{ik}(p,t)$ converge absolutely and uniformly for $t \in N$. Thus $S_i(p,t)$ and $f_{ik}(p,t)$ are holomorphic functions on $U_i \times N$ and $U_i \cap U_k \times N$, respectively, and satisfy (11), (12), (12a), (13). This completes our proof of Theorem 1.

THEOREM 2. *Let* $\mathfrak{V} \xrightarrow{\varpi} M$ *be a complex analytic family of compact submanifolds of* W, *where* M *is a spherical domain on the space of* m *complex variables* $t_1, t_2, \cdots, t_m$ *with the center* 0. *If* $\rho_{d,0}\colon T_0 \to H^0(V_0, \Psi_0)$ *is bijective, then* $\rho_{d,t}\colon T_t \to H^0(V_t, \Psi_t)$ *is bijective for each point* t *in a sufficiently small neighborhood* N *of* 0 *on* M.

Proof. Let $\psi_r(t) = \rho_{d,t}(\partial/\partial t_r)$, $r = 1, 2, \cdots, m$. By hypothesis, $\{\psi_1(0), \psi_2(0), \cdots, \psi_m(0)\}$ forms a base of $H^0(V_0, \Psi_0)$. It follows that $\psi_1(t), \psi_2(t), \cdots, \psi_m(t)$ are linearly independent for $t \in N$, while we have

$$\dim H^0(V_t, \Psi_t) \leqq \dim H^0(V_0, \Psi_0), \qquad \text{for } t \in N. \tag{45}$$

Consequently, $\{\psi_1(t), \psi_2(t), \cdots, \psi_m(t)\}$ forms a base of $H^0(V_t, \Psi_t)$ for $t \in N$. This proves our Theorem 2. We remark that the above inequality (45), a special case of the theorem of upper semi-continuity, can easily be derived from the classical theorem to the effect that any family of uniformly bounded holomorphic functions is a normal family.

5. Maximal families; proof of main theorem. First we prove the following

THEOREM 3. *Let* $\mathfrak{V} \xrightarrow{\varpi} M$ *be a complex analytic family of compact submanifolds of* W *(of codimension* 1*). If* $\rho_{d,t}\colon T_t \to H^0(V_t, \Psi_t)$ *is bijective for a point* t *of* M, *then the family* $\mathfrak{V} \xrightarrow{\varpi} M$ *is maximal at the point* t.

Proof. Suppose that $M = \{t \mid \sum_{r=1}^{m} |t_r|^2 < 1\}$ and that $\rho_{d,0}\colon T \to H^0(V_0, \Psi_0)$ is bijective. Moreover, let $\mathfrak{V}' \xrightarrow{\varpi'} M'$ be an arbitrary complex analytic family of compact submanifolds of W such that $\varpi'^{-1}(0) = V_0$, where

$$M' = \{s \mid \sum_{r=1}^{l} |s_r|^2 < 1\},$$

and let $N' = \{s \mid \sum_{r=1}^{l} |s_r|^2 < \delta\}$ be a sufficiently small spherical subdomain of M'. Our purpose is to construct a holomorphic map $h\colon s \to t = h(s)$ of N' into M with $h(0) = 0$ such that $\varpi'^{-1}(s) = \varpi^{-1}(h(s))$.

Let $U_i, w_i(p), \cdots$ have the same meaning as in Section 3 and let $\{S_i(p,t)\}$, $\{f_{ik}(p,t)\}$ be the systems of holomorphic functions $S_i(p,t)$, $f_{ik}(p,t)$, defined respectively on $U_i \times M$, $U_i \cap U_k \times M$, which determine the complex analytic family $\mathfrak{V} \subset W \times M$ in the manner described in Section 2. Moreover, let $\{R_i(p,s)\}$, $\{e_{ik}(p,s)\}$ be the corresponding systems which determine $\mathfrak{V}' \subset W \times M'$. We have therefore

$$\left\{\begin{aligned} S_i(p,t) &= f_{ik}(p,t) S_k(p,t), \\ R_i(p,s) &= e_{ik}(p,s) R_k(p,s). \end{aligned}\right. \tag{46}$$

In this Section we are exclusively concerned with neighborhoods U_i which meet V_0. Obviously, we may assume that

$$S_i(p,0) = R_i(p,0) = w_i(p),$$

$$f_{ik}(p,0) = e_{ik}(p,0) = f_{ik|0}(p).$$

By means of $S_i(p,t)$ and $R_i(p,s)$, the condition $\varpi'^{-1}(s) = \varpi^{-1}(h(s))$ can be formulated as follows: There exist non-vanishing holomorphic functions $f_i(p,s)$ defined respectively on $U_i \times N'$ such that

$$(47) \qquad f_i(p,s)R_i(p,s) = S_i(p,h(s)), \qquad \text{for } p \in U_i, s \in N'.$$

We write $h(s)$ in the form

$$h(s) = (h_1(s), \cdots, h_r(s), \cdots, h_m(s))$$

and expand each component $h_r(s)$ into power series

$$h_r(s) = \sum_{\mu=1}^{\infty} h_{r|\mu}(s),$$

where $h_{r|\mu}(s)$ is a homogeneous polynomial of degree μ in s. Moreover, let

$$h^\mu{}_r(s) = h_{r|1}(s) + h_{r|2}(s) + \cdots + h_{r|\mu}(s),$$
$$h^\mu(s) = (h^\mu{}_1(s), \cdots, h^\mu{}_r(s), \cdots, h^\mu{}_m(s)).$$

Similarly, let

$$f_i(p,s) = 1 + \sum_{\mu=1}^{\infty} f_{i|\mu}(p,s),$$

where $f_{i|\mu}(p,s)$ is a homogeneous polynomial of degree μ in s, and let

$$f^\mu{}_i(p,s) = 1 + f_{i|1}(p,s) + \cdots + f_{i|\mu}(p,s).$$

For any holomorphic functions $P(s)$, $Q(s)$ in $s = (s_1, s_2, \cdots, s_l)$, we indicate by $P(s) \underset{\mu}{\equiv} Q(s)$ that the power series expansion of $P(s) - Q(s)$ in $s_1, s_2, \cdots, s_l$ contains no terms of degree $\leqq \mu$. Clearly, (47) is equivalent to the system of congruences

$$(48)_\mu \qquad f^\mu{}_i(p,s)R_i(p,s) \underset{\mu}{\equiv} S_i(p,h^\mu(s)), \qquad (\mu = 0,1,2,\cdots).$$

In what follows we denote by $\bar{f}^{\mu-1}{}_i(p,s), \bar{R}_i(p,s), \bar{S}_i(p,t), \cdots$ the restrictions of the functions $f^{\mu-1}{}_i(p,s), R_i(p,s), S_i(p,s), \cdots$ to V_0. We expand $S_i(p,t)$ into the power series

$$S_i(p,t) = w_i(p) + S_{i|1}(p,t) + S_{i|2}(p,t) + \cdots$$

and let

$$(49) \qquad S_{i|1}(p,t) = \sum_{r=1}^{m} B_{ir}(p)t_r.$$

The restrictions $\beta_{ir}(p) = \bar{B}_{ir}(p)$ satisfy

$$\beta_{ir}(p) = f_{ik|0}(p)\beta_{kr}(p), \qquad \text{for } p \in V_0 \cap U_i \cap U_k;$$

thus $\{\beta_{ir}(p)\}$ represents an element β_r of $H^0(V_0, \Psi_0)$. In fact, β_r is the infinitesimal displacement $-\rho_{d,0}(\partial/\partial t_r)$. Since, by hypothesis, $\rho_{d,0}$: $T_0 \to H^0(V_0, \Psi_0)$ is bijective, $\{\beta_1, \cdots, \beta_r, \cdots, \beta_m\}$ forms a base of $H^0(V_0, \Psi_0)$.

Now we construct $h^\mu(s)$ and $f^\mu{}_i(p,s)$ satisfying $(48)_\mu$ by induction on μ.

For $\mu=0$ the congruence $(48)_0$ is obvious. Assume therefore that $h^{\mu-1}(s)$ and $f^{\mu-1}{}_i(p,s)$ satisfying $(48)_{\mu-1}$ are already determined. Then we can determine homogeneous polynomials $\Gamma_{i|\mu}(p,s)$ of degree μ in s by

$$(50) \qquad \Gamma_{i|\mu}(p,s) \underset{\mu}{\equiv} f^{\mu-1}{}_i(p,s)R_i(p,s) - S_i(p,h^{\mu-1}(s)).$$

The coefficients of $\Gamma_{i|\mu}(p,s)$ are holomorphic functions in p defined on U_i. The restrictions $\bar{\Gamma}_{i|\mu}(p,s)$ of $\Gamma_{i|\mu}(p,s)$ satisfy

$$(51) \qquad \bar{\Gamma}_{i|\mu}(p,s) = f_{ik|0}(p)\bar{\Gamma}_{k|\mu}(p,s), \qquad \text{for } p\in V_0\cap U_i\cap U_k.$$

To prove this we remark that

$$(52) \qquad f^{\mu-1}{}_i(s)e_{ik}(s) \underset{\mu-1}{\equiv} f_{ik}(h^{\mu-1}(s))f^{\mu-1}{}_k(s),$$

where we omit the variable p for simplicity. In fact, combinging $(48)_{\mu-1}$ with (46), we obtain

$$\begin{aligned} f^{\mu-1}{}_i(s)e_{ik}(s)R_k(s) &= f^{\mu-1}{}_i(s)R_i(s) \underset{\mu-1}{\equiv} S_i(h^{\mu-1}(s)) \\ &= f_{ik}(h^{\mu-1}(s))S_k(h^{\mu-1}(s)) \underset{\mu-1}{\equiv} f_{ik}(h^{\mu-1}(s))f^{\mu-1}{}_k(s)R_k(s). \end{aligned}$$

This proves (52). Since $\bar{R}_k(s) \underset{0}{\equiv} 0$, we get from (52) the congruence

$$\bar{f}^{\mu-1}{}_i(s)\bar{R}_i(s) = \bar{f}^{\mu-1}{}_i(s)\bar{e}_{ik}(s)\bar{R}_k(s) \underset{\mu}{\equiv} \bar{f}_{ik}(h^{\mu-1}(s))\bar{f}^{\mu-1}{}_k(s)\bar{R}_k(s).$$

Hence we have

$$\bar{f}^{\mu-1}{}_i(s)\bar{R}_i(s) - \bar{S}_i(h^{\mu-1}(s)) \underset{\mu}{\equiv} \bar{f}_{ik}(h^{\mu-1}(s))\{\bar{f}^{\mu-1}{}_k(s)\bar{R}_k(s) - \bar{S}_k(h^{\mu-1}(s))\}.$$

Combining this with (50), we obtain

$$\Gamma_{i|\mu}(p,s) \underset{\mu}{\equiv} \bar{f}_{ik}(p,h^{\mu-1}(s))\bar{\Gamma}_{k|\mu}(p,s) \underset{\mu}{\equiv} \bar{f}_{ik|0}(p)\bar{\Gamma}_{k|\mu}(p,s).$$

This proves (51).

Since $h^\mu{}_r(s) = h^{\mu-1}{}_r(s) + h_{r|\mu}(s)$, the congruence $(48)_\mu$ is rewritten in in the form

$$w_i f_{i|\mu}(s) + f^{\mu-1}{}_i(s)R_i(s) \underset{\mu}{\equiv} S_i(h^{\mu-1}(s)) + \sum_{r=1}^{m} B_{ir}(p)h_{r|\mu}(s).$$

We infer therefore that $(48)_\mu$ is equivalent to

$$(53) \qquad \sum_{r=1}^{m} B_{ir}(p)h_{r|\mu}(s) = w_i(p)f_{i|\mu}(p,s) + \Gamma_{i|\mu}(p,s).$$

The restriction of (53) to V_0 gives the equality

$$(54) \qquad \sum_{r=1}^{m} \beta_{ir}(p)h_{r|\mu}(s) = \bar{\Gamma}_{i|\mu}(p,s).$$

Now (51) shows that $\{\bar{\Gamma}_{i|\mu}(p,s)\}$ represents a homogeneous polynomial degree μ in s *with coefficients in* $H^0(V_0,\Psi_0)$. It follows that there exist ›mogeneous polynomials $h_{r|\mu}(s)$ of degree μ in s with constant coefficients tisfying (54). We define homogeneous polynomials $f_{i|\mu}(p,s)$ by

$$f_{i|\mu}(p,s) = \{\sum_{r=1}^{m} B_{ir}(p)h_{r|\mu}(s) - \Gamma_{i|\mu}(p,s)\}/w_i(p). \tag{5}$$

e infer readily from (54) that the coefficients of $f_{i|\mu}(p,s)$ are holomorphic nctions in p defined on U_i, while it is clear that the $f_{i|\mu}(p,s)$ satisfy (53). his completes our inductive construction of $h^{\mu}(s)$ and $f^{\mu}{}_i(p,s)$ satisfying 8)$_\mu$. We note that $h^{\mu}(s)$ and $f^{\mu}{}_i(p,s)$ are *uniquely* determined. For our ırpose it suffices to show that the power series $h_r(s)$, $f_i(p,s)$ thus deter- ined converge absolutely and uniformly for $s \in N'$, provided that the spherical ›main N' is sufficiently small.

We prove by induction on μ the estimates

$$h^{\mu}{}_r(s) \ll A(s), \tag{6)$_\mu$}$$

$$f^{\mu}{}_i(p,s) - 1 \ll A(s), \tag{7)$_\mu$}$$

nere

$$A(s) = (b/64c)\sum_{\mu=1}^{\infty} c^{\mu}(s_1+s_2+\cdots+s_l)^{\mu}/\mu^2$$

ovided that the constants b and c are chosen properly. We have

$$A(s)^2 \ll (b/c)A(s)$$

f. (28)) and therefore

$$A(s)^{\nu} \ll (b/c)^{\nu-1}A(s), \qquad \text{for } \nu = 2,3,4,\cdots. \tag{8}$$

e choose a constant $a > 0$ such that

$$S_i(p,t) - w_i(p) \ll \sum_{\nu=1}^{\infty} a^{\nu}(t_1+t_2+\cdots+t_m)^{\nu}, \tag{9}$$

$$R_i(p,s) - w_i(p) \ll \sum_{\nu=1}^{\infty} a^{\nu}(s_1+\cdots+s_l)^{\nu}/64\nu^2. \tag{0}$$

Now $(56)_1$ and $(57)_1$ are obvious provided that b is sufficiently large. ssume therefore that $(56)_{\mu-1}$ and $(57)_{\mu-1}$ are already proved. We first timate

$$\Gamma_{i|\mu}(p,s) \underset{\mu}{\equiv} f^{\mu-1}{}_i(p,s)R_i(p,s) - S_i(p,h^{\mu-1}(s)).$$

nce $\Gamma_{i|\mu}(p,s)$ is a homogeneous polynomial of degree μ in s, the terms ${}^{-1}{}_i(p,s)w_i(p)$ and $w_i(p) + S_{i|1}(p,h^{\mu-1}(s))$ contribute nothing to $\Gamma_{i|\mu}(p,s)$.

Hence we get

$$\Gamma_{i|\mu}(p,s) \ll (A(s)+1)\sum_{\nu=1}^{\infty} a^\nu s^\nu/64\nu^2 + \sum_{\nu=2}^{\infty} a^\nu (mA(s))^\nu,$$

where $s^\nu = (s_1+s_2+\cdots+s_l)^\nu$. Suppose that

$$c \geqq 2mab, \qquad b > 1.$$

Then we have

$$\sum_{\nu=1}^{\infty} a^\nu s^\nu/64\nu^2 \ll (a/64c)\sum_{\nu=1}^{\infty} c^\nu s^\nu/\nu^2 = (a/b)A(s)$$

and therefore, by (58),

$$(A(s)+1)\sum_{\nu=1}^{\infty} a^\nu s^\nu/64\nu^2 \ll ((a/c)+(a/b))A(s).$$

Moreover, using (58), we get

$$\sum_{\nu=2}^{\infty} a^\nu (mA(s))^\nu \ll A(s)\sum_{\nu=2}^{\infty} a^\nu m^\nu b^{\nu-1}/c^{\nu-1} \ll (2m^2a^2b/c)A(s).$$

Thus we obtain

$$\Gamma_{i|\mu}(p,s) \ll c_5 A(s), \tag{61}$$

where

$$c_5 = (a/c)+(a/b)+(2m^2a^2b/c).$$

In view of (54), there exists a constant κ which is independent of μ such that (61) implies

$$h_{r|\mu}(s) \ll \kappa c_5 A(s).$$

Finally, since the coefficients of $f_{i|\mu}(p,s)$ are holomorphic on the polycylinder U_i defined by $|w_i(p)|<1$, $|z^1_i(p)|<1,\cdots,|z^n_i(p)|<1$, we infer from (55) that

$$f_{i|\mu}(p,s) \ll (ma\kappa+1)c_5A(s)$$

(note that (59) implies $|B_{ir}(p)|<a$). Consequently, by choosing the constants b and c properly, we obtain

$$h_{r|\mu}(s) \ll A(s),$$
$$f_{i|\mu}(p,s) \ll A(s).$$

This completes our inductive proof of $(56)_\mu$ and $(57)_\mu$, and the convergence of $h_r(s)$, $f_i(p,s)$ for $s \in N'$ follows.

Now it is clear that our main theorem follows from Theorems 1, 2 and 3.

6. Proof of Lemma 2. For simplicity, we write U_i for $V_0 \cap U_i$ and denote by $\mathfrak{U}$ the covering $\{U_i\}$ of V_0. For any 0-cochain $\phi = \{\phi_i(p)\}$, 1-cochain $\psi = \{\psi_{ik}(p)\}, \cdots$ on $\mathfrak{U}$ with coefficients in the sheaf Ψ_0, we define the norms of $\phi, \psi, \cdots$ by

$$\| \phi \| = \max_i \sup_{p \in U_i} | \phi_i(p) |,$$

$$\| \psi \| = \max_{i,k} \sup_{p \in U_i \cap U_k} | \psi_{ik}(p) |,$$

$$\cdots.$$

The coboundary $\delta\phi$ of ϕ is defined by

$$(\delta\phi)_{ik}(p) = f_{ik|0}(p)\phi_k(p) - \phi_i(p), \qquad p \in U_i \cap U_k.$$

Our purpose is to show the existence of a constant c_4 having the following properties: *If ψ is the coboundary of a 0-cochain, then we can find a 0-cochain ϕ with $\delta\phi = \psi$ such that*

$$\| \phi \| \leqq c_4 \| \psi \|. \tag{62}$$

For any ψ which is the coboundary of a 0-cochain, we define

$$\iota(\psi) = \inf_{\delta\phi = \psi} \| \phi \|.$$

It suffices to prove the existence of a constant c such that

$$\iota(\psi) \leqq c \| \psi \|. \tag{63}$$

Assume that such a constant c does not exist. Then we find a sequence $\psi', \psi'', \cdots, \psi^{(\mu)}, \cdots$ such that

$$\iota(\psi^{(\mu)}) = 1, \qquad \| \psi^{(\mu)} \| < 1/\mu.$$

The equality $\iota(\psi^{(\mu)}) = 1$ implies that there exists $\phi^{(\mu)}$ with $\delta\phi^{(\mu)} = \psi^{(\mu)}$ satisfying

$$\| \phi^{(\mu)} \| < 2.$$

We take a covering $\{U^*_i\}$ of V_0 by *compact* subsets $U^*_i \subset U_i$. Moreover, we write each $\phi^{(\mu)}$ explicitly in the form $\{\phi_i^{(\mu)}(p)\}$. Since $| \phi_k^{(\mu)}(p) | < 2$ for $p \in U_k$, there exists a subsequence $\phi^{(\mu_1)}, \phi^{(\mu_2)}, \cdots, \phi^{(\mu_\nu)}$ of $\phi', \phi'', \cdots$ such that $\phi_k^{(\mu_\nu)}(p)$ converges absolutely and uniformly on U^*_k for each k. On the other hand, it follows from $\| \delta\phi^{(\mu)} \| = \| \psi^{(\mu)} \| < 1/\mu$ that

$$| f_{ik|0}(p)\phi_k^{(\mu)}(p) - \phi_i^{(\mu)}(p) | < 1/\mu, \qquad \text{for } p \in U_i \cap U_k. \tag{64}$$

Since any point $p \in U_i$ is covered by at least one U^*_k, we infer from (64)

that $\phi_i^{(\mu_\nu)}(p)$ converges absolutely and uniformly on the whole neighborhood U_i. Let $\phi_i(p) = \lim_\nu \phi_i^{(\mu_\nu)}(p)$ and let $\phi = \{\phi_i(p)\}$. Then we have

$$\| \phi^{(\mu_\nu)} - \phi \| \to 0 \qquad (\nu \to \infty),$$

while it follows from (64) that $\delta\phi = 0$ and therefore $\delta(\phi^{(\mu_\nu)} - \phi) = \psi^{(\mu_\nu)}$. This contradicts with $\iota(\psi^{(\mu_\nu)}) = 1$.

INSTITUTE FOR ADVANCED STUDY
AND
PRINCETON UNIVERSITY.

REFERENCES.

[1] H. Cartan, "Variétés analytiques complexes et cohomologie," *Colloque sur les fonctions des plusieurs variables tenu à Bruxelles*, 1953, pp. 41-55. Georges Thone, Liège; Masson et Cie, Paris, 1953.

[2] K. Kodaira, "Some results in the transcendental theory of algebraic varieties," *Annals of Mathematics*, vol. 59 (1954), pp. 86-134.

[3] ———, "Characteristic linear systems of complete continuous systems," *American Journal of Mathematics*, vol. 78 (1956), pp. 716-744.

[4] ——— and D. C. Spencer, "On deformations of complex analytic structures, I, II," *Annals of Mathematics*, vol. 67 (1958), pp. 328-466.

[5] J. Leray, "L'anneau spectral et l'anneau filtré d'homologie d'un espace localement compact et d'une application continue," *Journal de Mathématiques Pures et Appliquées*, vol. 29 (1950), pp. 1-139.

[6] F. Severi, "Sulla teoria degl'integrali semplici di 1a specie appartenenti ad una superficie algebrica," *Rendiconti della Reale Accademi Nazionale dei Lincei*, s. V, vol. XXX (1921), seven notes: i) pp. 163-167; ii) pp. 204-208; iii) pp. 231-235; iv) pp. 276-280; v) 296-301; vi) pp. 328-332; vii) pp. 365-367.

[7] ———, "Sul teorema fondamentale dei sistemi continui di curve," *Annali di Matematica*, s. IV, vol. XXIII (1944), pp. 149-181.

[8] ———, "La géométrie algébrique itallienne. Sa rigueur, ses méthodes, ses problèmes," *Colloque de géométrie algébrique*, Liège, 1949, pp. 9-55.

[9] H. Poincaré, "Sur les courbes tracées sur les surfaces algébriques," *Annales École Normale Supérieure*, III s., vol. 27 (1910), pp. 55-108.

[10] ———, "Sur les courbes tracées sur les surfaces algébriques," *Sitzungsberichte der Berliner mathematischen Gesellschaft*, vol. 10 (1911), pp. 28-55.

[11] A. Weil, "On Picard varieties," *American Journal of Mathematics*, vol. 74 (1952), pp. 865-894.

[12] O. Zariski, "Algebraic surfaces," *Ergebnisse der Mathematik und Ihrer Grenzgebiete*, Bd. 5, No. 5, 1935.

AN EXAMPLE TO A PROBLEM OF ABHYANKAR.*

By MASAYOSHI NAGATA.

In the paper of Abhyankar, "On the field of definition of a non-singular birational transform of an algebraic surface," *Annals of Mathematics*, vol. 65, No. 2 (1957), the following question was asked:

Let K be a function field of dimension 2 over an imperfect ground field k of characteristic p ($\neq 0$) and let k' be a purely inseparable extension of k of degree p. Let K' be the field generated by K over k'. Let R be a normal spot of K over k and let R' be the derived normal ring of R in K'. Assume that R' is a regular local ring. Is then R regular?

In the present note, we shall show an example where R is not regular. In fact, we shall give an example of such pair (R, R') with the following additional conditions:

$\mathfrak{m}$ and $\mathfrak{m}'$ being the maximal ideals of R and R' respectively, (i) $\mathfrak{m}R' = \mathfrak{m}'$ and (ii) $[R'/\mathfrak{m}' : R/\mathfrak{m}] = p^2$ $(> [K' : K])$.

Let k be a field of characteristic $p \neq 0$ which has elements u and v such that $[k(u^{1/p}, v^{1/p}) : k] = p^2$. Let x and y be variables over k and let z be a root of the polynomial $Z^p + yZ + u + v^{1/p}x$. Set $w = v^{1/p}x + zy$. We shall show that the pair of $R = k[x, y, w]_{(x,y,w)}$ and $R' = k(v^{1/p})[x, y, z]_{(x,y)}$ (observe that $Z^p + u$ is irreducible over $k(v^{1/p})$ and therefore x and y generate a maximal ideal of $k(v^{1/p})[x, y, z]$) is the required example.

Let K and K' be the field of quotients of R and R' respectively. Then we see that $K' = K(v^{1/p})$. R' is obviously a regular local ring. Since z modulo $(x, y) = u^{1/p}$, the residue class field of R' is $k(u^{1/p}, v^{1/p})$. Therefore we see that the condition (ii) above is satisfied by R and R'; (i) is obviously satisfied. Therefore we have only to prove the normality of R.

Since $w = v^{1/p}x + zy$, we have $z = (w - v^{1/p})/y$. Since $z^p + yz + u + v^{1/p}x = 0$, i.e., $z^p + u + w = 0$, we have $w^p + y^p w + (uy^p - vx^p) = 0$, which is

* Received May 12, 1958.

the irreducible monic equation for w over $k[x, y]$. Therefore, by the mixed Jacobian criterion for simplicity due to Zariski, we see that R is the only one singular spot of the affine model defined by $k[x, y, w]$, which shows the normality of R. Thus the proof is completed.

Remark. If we want to construct similar examples without requiring that K is a regular extension of k, then the following construction gives a much simpler example than above:

With the same k, u, v, x and y as above, set $z = u^{1/p}x + v^{1/p}y$. Then $R = k[x, y, z]_{(x,y,z)}$ and $R' = k(u^{1/p}, v^{1/p})[x, y]_{(x,y)}$ give a required pair.

HARVARD UNIVERSITY AND
KYOTO UNIVERSITY.

ON THE UNIQUENESS OF THE CAUCHY PROBLEM FOR PARABOLIC EQUATIONS.*[1]

By Avner Friedman.

Introduction. Consider the second order parabolic equation

$$\partial u/\partial t = Lu \tag{0.1}$$

in the strip

$$0 < t < d, \qquad x = (x_1, \cdots, x_n), \qquad -\infty < x_i < \infty. \tag{0.2}$$

Tychonoff [13] constructed a solution of (0.1) which vanishes on $t = 0$ but is not identically zero; thus there is no uniqueness of the Cauchy problem. However, if a solution $u(x,t)$ of (0.1) satisfies the growth condition

$$u(x,t) = O(\exp\{K\,|\,x\,|^2\}) \qquad (K \geqq 0) \tag{0.3}$$

and if it vanishes on $t = 0$, then it vanishes identically in the strip (0.2). The proof of this theorem for the heat equation was given by Tychonoff [13]. It was extended to general second order parabolic equations by Krzyzański [5] (see also [6]). It was then extended to parabolic systems of order $2m$ provided (0.3) is replaced by

$$u(x,t) = O(\exp\{K\,|\,x\,|^{2m/(2m-1)}\}) \qquad (K \geqq 0). \tag{0.4}$$

In the case where the coefficients depend only on t it was proved by Ladyzhenskaya [7] (for $K = 0$ it was proved by Petrowski [9]). In the general case it was proved by Eidelman [4; p. 73] (see also [3]). Slobodetski [12] announced that if the coefficients of the parabolic system depend only on t, then uniqueness holds under the assumption

$$\int\int \exp\{-K\,|\,x\,|^{2m/(2m-1)}\}\,|\,u(x,t)\,|\,dxdt < \infty \qquad (K > 0) \tag{0.5}$$

which is weaker than the assumption (0.4). (The integration in (0.5) is taken over the strip (0.2).)

* Received July 17, 1958; Revised November 21, 1958.

[1] Prepared under ONR Contract Nonr-222(37) (NR 041 157) with the University of California in Berkeley.

Another type of assumption sufficient to ensure uniqueness was obtained by Widder [14]. He proved in case of the heat equation that a solution satisfying

$$u(x,t) \geqq 0 \tag{0.6}$$

and vanishing for $t=0$ must vanish identically. Assumption (0.6) seems to be more natural than assumption (0.3) since temperatures are always nonnegative. Serrin [11] announced an extension of Widder's result to solutions of the equation

$$u_t = a(x) u_{xx} + b(x) u_x + c(x) u \tag{0.7}$$

with Hölder continuous and uniformly bounded coefficients and with $a(x) \geqq \text{const.} > 0$.

In this paper we extend all the above-mentioned results. We first consider general second order parabolic equations and prove uniqueness (i) under the assumption (0.5) with $m=1$, and (ii) under the assumption (0.6). Then we consider general parabolic systems and furnish the tools for the proof of the uniqueness of the Cauchy problem under the assumption (0.5).

1. Statement of uniqueness theorems for second order equations. Consider the equation

$$\partial u/\partial t = Lu \equiv \sum_{i,j=1}^{n} a_{ij}(x,t)\partial^2 u/\partial x_i \partial x_j + \sum_{i=1}^{n} b_i(x,t)\partial u/\partial x_i + c(x,t)u, \tag{1.1}$$

where $x=(x_1,\cdots,x_n)$ varies in the whole n-dimensional Euclidean space E_n and $0<t<d$. Denote by D the topological product of E_n with the interval $0<t<d$. We shall make on L the following assumptions:

(A) L is uniformly elliptic in $\bar{D}$ (the closure of D), that is, there exists a positive constant K such that for all $(x,t) \in \bar{D}$ and for every real vector $\xi = (\xi_1,\cdots,\xi_n)$

$$\sum_{i,j=1}^{n} a_{ij}(x,t)\xi_i\xi_j \geqq K \sum_{i=1}^{n} \xi_i^2. \tag{1.2}$$

(B) The functions

$$a_{ij},\ (\partial/\partial x_\lambda)a_{ij},\ (\partial^2/\partial x_\lambda \partial x_\mu)a_{ij},\ (\partial/\partial t)a_{ij},\ b_i,\ (\partial/\partial x_\lambda)b_i,\ c \tag{1.3}$$

are locally Hölder continuous and uniformly bounded in $\bar{D}$; denote by K' a bound on these functions.

By a solution of (1.1) in D is meant a function $u(x,t)$ which is con-

tinuous in $\bar{D}$ and which has continuous partial derivatives $\partial u/\partial x_i$, $\partial^2/\partial x_i \partial x_j$, $\partial u/\partial t$ in D satisfying (1.1).

THEOREM 1. *Let L satisfy the assumptions* (A), (B). *If $u(x,t)$ is a solution of* (1.1) *in the strip D which satisfies the growth condition*

$$\int_0^d \int_{E_n} \exp\{-H_0 |x|^2\} |u(x,t)| \, dx dt < \infty \qquad (H_0 > 0) \tag{1.4}$$

and if $u(x,0) \equiv 0$ for $x \in E_n$, then $u(x,t) \equiv 0$ in D.

THEOREM 2. *Let L satisfy the assumptions* (A), (B). *If $u(x,t)$ is a nonnegative solution of* (1.1) *in the strip D and if $u(x,0) \equiv 0$ for $x \in E_n$, then $u(x,t) \equiv 0$ in D.*

2. Proof of Theorem 1. We shall make use of the fundamental solution $\Gamma(x,t;\xi,\tau)$ $(t > \tau)$ of (1.1) defined in the whole strip $\bar{D}$, which was constructed by Dressel [2] under the assumptions (A), (B). As a function of (x,t) it satisfies the equation $\partial\Gamma/\partial t = L\Gamma$ and as a function of (ξ,τ) it satisfies the adjoint equation $\partial\Gamma/\partial\tau = -L^*\Gamma$, where

$$L^* v = \sum_{i,j=1}^{n} (\partial^2/\partial x_i \partial x_j)(a_{ij} v) - \sum_{i=1}^{n} (\partial/\partial x_i)(b_i v) + cv.$$

Γ can be written in the form

$$\Gamma(x,t;\xi,\tau) = Z(x,t;\xi,\tau)[1 + O((t-\tau)^{\frac{1}{2}})] \tag{2.1}$$

(making use of the explicit form of Γ and of [2; Lemma 2]), where

$$\begin{aligned} Z(x,t;\xi,\tau) & \\ &= \begin{cases} [F(\xi,\tau)(t-\tau)^{n/2}]^{-1} \exp\{-\sigma(x,t;x-\xi)/4(t-\tau)\} & \text{if } t > \tau \\ 0 \text{ if } t < \tau. \end{cases} \end{aligned} \tag{2.2}$$

Here, $\sigma(x,t;x-\xi) = \sum A_{ij}(x,t)(x_i - \xi_i)(x_j - \xi_j)$, (A_{ij}) is the matrix inverse to (a_{ij}), and $F(\xi,\tau)$ is a certain positive function depending on σ (see [1; p. 191]).

Later on we shall need the fact that $\Gamma(x,t;\xi,\tau) > 0$ if $t > \tau$. For $t-\tau$ sufficiently small this follows from (2.1). Noting now that $\Gamma(x,t;\xi,\tau) \to 0$ as $|x| \to \infty$, uniformly with respect to t, and recalling that $\Gamma(x,\tau+\epsilon,\xi,\tau) > 0$ if ϵ is positive and sufficiently small, we apply the maximum principle [8] and thus conclude that $\Gamma(x,t;\xi,\tau)$ is a positive function for $t > \tau$. We finally mention that for any $i = 1,\cdots,n$,

$$|\partial\Gamma(x,t;\xi,\tau)/\partial x_i| = |\partial Z(x,t;\xi,\tau)/\partial x_i| \, [1 + O((t-\tau)^{\frac{1}{2}})]; \tag{2.3}$$

the constants in $O((t-\tau)^{\frac{1}{2}})$ both in (2.1) and in (2.3) depend only on K, K'.

It is enough (in both Theorems 1 and 2) to prove that $u(x,t)\equiv 0$ for $x\in E_n$, $0\leqq t<\eta$ for some positive η, since then we can carry out the same argument step by step. Later on whe shall make use of the fact that η may be taken to be sufficiently small.

Let $(\bar{x},\bar{t})$ be an arbitrary fixed point in the strip $0<t<\eta$. If we prove that $u(\bar{x},\bar{t})=0$ then, by the previous remark, the proof of Theorem 1 is completed. Denote by B_R the sphere in E_n with center $\bar{x}$ and radius R and denote by B'_R the domain $B_{R+1}-B_R$. Let $h(\xi)$ be a twice continuously differentiable function in E_n satisfying the following properties:

$$(2.4)\qquad h(\xi)=\begin{cases}1 \text{ if } 0\leqq|\xi|\leqq R\\ 0 \text{ if } R+1\leqq|\xi|<\infty\end{cases}$$

$$(2.5)\qquad 0\leqq h(\xi)\leqq 1 \text{ and } \sum_i|\partial h(\xi)/\partial\xi_i|+\sum_{i,j}|\partial^2 h(\xi)/\partial\xi_i\partial\xi_j|\leqq A \quad \text{for } R<|\xi|<R+1,$$

where A is an appropriate universal constant.

Integrating Green's identity

$$(2.6)\qquad \begin{aligned} &v(Lw-\partial w/\partial\tau)-w(L^*v+\partial v/\partial\tau)\\ &=\sum_{i=1}^n(\partial/\partial\xi_i)\Big[\sum_{k=1}^n(va_{ik}\partial w/\partial\xi_k-wa_{ik}\partial v/\partial\xi_k-vw\partial a_{ik}/\partial\xi_k)+b_iwv\Big]\\ &\quad-(\partial/\partial\tau(wv)\end{aligned}$$

with $w=u(\xi,\tau)$, $v=h(\xi)\Gamma(\bar{x},\bar{t};\xi,\tau)$ over the whole strip $0<\tau<\bar{t}-\epsilon(\epsilon>0)$ and taking $\epsilon\to 0$ we get, on using the properties of h, Γ and the assumption $u(\xi,0)\equiv 0$,

$$(2.7)\qquad u(\bar{x},\bar{t})=\int_0^{\bar{t}}\int_{B'_R}u[L^*(h\Gamma)+\partial(h\Gamma)/\partial\tau]\,d\xi d\tau.$$

Since $L^*(h\Gamma)+\partial(h\Gamma)/\partial\tau$ involves only linear combinations of Γ and $\partial\Gamma/\partial\xi_i$ with coefficients which (by (2.5) and assumption (B)) are bounded by a constant independent of R, we can easily estimate the right side of (2.7), making use of (2.1), (2.2), (2.3). We get

$$(2.8)\qquad |u(\bar{x},\bar{t})|\leqq A\exp\{-HR^2/\eta\}\int_0^{\bar{t}}\int_{B'_R}|u(\xi,\tau)|\,d\xi d\tau,$$

where A, H are positive constants depending only on K, K'.

We now note that (1.4) implies

$$(2.9)\qquad \int_0^{\bar{t}}\int_{E_n}\exp\{-2H_0|\xi-\bar{x}|^2\}\,|u(\xi,\tau)|\,d\xi d\tau<\infty.$$

Hence,

$$\int_0^{\bar t}\int_{B'_R}\exp\{-2H_0\,|\,\xi-\bar x\,|^2\}\,|\,u(\xi,\tau)\,|\,d\xi d\tau\to 0 \text{ as } R\to\infty. \tag{2.10}$$

Taking η to satisfy $H/\eta > 2H_0$, then letting $R\to\infty$ in (2.8) and using (2.10), we conclude that $u(\bar x,\bar t)=0$ and the proof is thereby completed.

3. Proof of Theorem 2. Without loss of generality we may assume that $c(x,t)\leqq 0$.

Consider the function

$$U_R(x,t)=\int_{|\xi|<R}\Gamma(x,t;\xi,\tau)u(\xi,\tau)\,d\xi, \tag{3.1}$$

where Γ is the fundamental solution of (1.1) in D, introduced in § 2. By [2] we conclude that

$$\lim_{t\to\tau+0}\ \sup_{x\to x^0} U_R(x,t)\leqq\begin{cases}u(x^0,\tau) & \text{if } |\,x^0\,|\leqq R\\ 0 & \text{if } |\,x^0\,|>R.\end{cases}$$

Hence, the function

$$v(x,t)=u(x,t)-U_R(x,t) \tag{3.2}$$

satisfies

$$\liminf v(x,t)\geqq 0 \tag{3.3}$$

as $t\to\tau+0$, $x\to x^0$. Furthermore, from the form of Γ we conclude that $U_R(x,t)\to 0$ as $|\,x\,|\to\infty$, uniformly with respect to t, $0\leqq t\leqq d$. Hence, (3.3) holds also when $|\,x\,|\to\infty$, uniformly with respect to t, $0\leqq t\leqq d$. Using the maximum principle [8], we easily conclude that $v(x,t)\geqq 0$ in D; more explicitly,

$$\int_{|\xi|<R}\Gamma(x,t;\xi,\tau)u(\xi,\tau)\,d\xi\leqq u(x,t) \text{ for } x\in E_n,\ t>\tau. \tag{3.4}$$

Noting that the left side of (3.4) is monotone increasing in R and taking $R\to\infty$, we get

$$\int_{E_n}\Gamma(x,t;\xi,\tau)u(\xi,\tau)\,d\xi\leqq u(x,t) \text{ for } x\in E_n, t>\tau \tag{3.5}$$

(the existence of the integral is implied).

Integrating both sides of (3.5) with respect to τ, $0<\tau<\eta$ and taking $x=0$, we obtain

$$\int_0^{\eta}\int_{E_n}\Gamma(0,t;\xi,\tau)u(\xi,\tau)\,d\xi d\tau\leqq\eta u(0,t). \tag{3.6}$$

any real vector $\sigma = (\sigma_1, \cdots, \sigma_n)$, the characteristic roots $\lambda = \lambda(\sigma)$ of the matrix $P_0(x, t, \sigma)$ satisfy the inequality $\operatorname{Re}\{\lambda\} < -\delta$.

(B′) The coefficients of the k-th derivatives which appear on the right side of (4.1) have derivatives of the first $k+1$ orders with respect to x, all being uniformly continuous with respect to (x, t) in D.

The assumptions (A′), (B′) are sufficient to ensure the existence of a fundamental solution to the system adjoint to (4.1) (see Eidelman [4; p. 71]). Denote it by $Z(x, t; \xi, \tau)$ $(t > \tau)$. As a function of (ξ, τ) it satisfies the system adjoint to (4.2). It also satisfies the inequalities

$$(4.3) \quad |(\partial/\partial\xi^i) Z(x, t; \xi, \tau)| \leqq \text{const.}/(t-\tau)^{(n+i)/2m}$$
$$\exp\{-\text{const.}\, |x-\xi|^{2m/(2m-1)}/(t-\tau)^{1/(2m-1)}\} \quad (i = 0, 1, \cdots, 2m),$$

where the constants are positive. Finally, for any continuous function $\phi(x, t)$ defined in $\bar{D}$ and for any bounded domain G in E_n,

$$(4.4) \qquad \lim_{\tau \to t-0} \int_G Z(x, t; \xi, \tau) \phi(\xi, \tau)\, d\xi = \phi(x, t).$$

Using these results, one can easily modify the proof of Theorem 1 and derive the following uniqueness theorem.

THEOREM 3. *Let the system* (4.1) *satisfy the assumptions* (A′), (B′). *If* $(u_1(x, t), \cdots, u_N(x, t))$ *is a solution of the system* (4.1) *in the strip* D *which satisfies the assumption*

$$(4.5) \qquad \int_0^d \int_{E_n} \exp\{-H_0 |x|^{2m/(2m-1)}\} |u_i(x, t)|\, dx dt < \infty$$
$$(i = 1, \cdots, N; H_0 > 0)$$

and if $u_i(x, 0) \equiv 0$ $(i = 1, \cdots, N)$ *for* $x \in E_n$, *then* $u_i(x, t) \equiv 0$ *for* $x \in E_n$, $0 \leqq t \leqq d$.

UNIVERSITY OF CALIFORNIA
AND
INDIANA UNIVERSITY.

REFERENCES.

[1] F. G. Dressel, "Fundamental solution of the parabolic equation," *Duke Mathematical Journal*, vol. 7 (1940), pp. 186-203.

[2] ———, "Fundamental solution of the parabolic equation, II," *ibid.*, vol. 13 (1946), pp. 61-70.

[3] S. D. Eidelman, "Estimates of solutions of parabolic systems and some of their applications," *Matematičeskiĭ Sbornik* (N. S.), vol. 33 (75) (1953), pp. 359-382.

[4] ———, "On fundamental solutions of parabolic systems," *ibid.*, vol. 38 (80) (1956), pp. 51-92.

[5] M. Krzyański, "Sur les solutions des équations du type parabolique déterminées dans une région illimitée," *Bulletin of the American Mathematical Society*, vol. 47 (1941), pp. 911-915.

[6] ———, "Sur les solutions de l'équation linéaire du type parabolique déterminées par les conditions initiales," *Annales de la Société Polonaise de Mathématique*, vol. 18 (1945), pp. 145-156.

[7] O. A. Ladyzhenskaya, "On the uniqueness of solutions of the Cauchy problem for linear parabolic equations," *Matematičeskiĭ Sbornik* (N. S), vol. 27 (69) (1950), pp. 175-184.

[8] L. Nirenberg, "A strong maximum principle for parabolic equations," *Communcations on Pure and Applied Mathematics*, vol. 6 (1953), pp. 167-177.

[9] I. G. Petrowski, "On the Cauchy problem for linear systems of partial differential equations in a domain of non-analytic functions," *Bull. d'Etat Moscow*, Ser. Inter., sect. A, vol. 1 (1938), pp. 1-72.

[10] D. Resch, "Temperature bounds on the infinite rod," *Proceedings of the American Mathematical Society*, vol. 3 (1952), pp. 632-634.

[11] J. B. Serrin, "A uniqueness theorem for the parabolic equation $u_t = a(x) u_{xx} + b(x) u_x + c(x) u$," *Bulletin of the American Mathematical Society*, vol. 60 (1954), p. 344.

[12] L. E. Slobodetski, "On the Cauchy problem for nonhomogeneous parabolic systems," *Doklady Akademii Nauk SSSR* (N. S), vol. 101 (1955), pp. 805-808.

[13] A. N. Tychonoff, "Theoremes d'unicite pour l'equation de la chaleur," *Matematičeskiĭ Sbornik* (N. S.), vol. 32 (1935), pp. 199-216.

[14] D. V. Widder, "Positive temperatures on the infinite rod," *Transactions of the American Mathematical Society*, vol. 55 (1944), pp. 85-95.

A RELATION BETWEEN *CW*-COMPLEXES AND FREE c. s. s. GROUPS.*

By Daniel M. Kan.

1. Introduction. The homotopy theory of c. s. s. complexes which satisfy the extension condition, the homotopy theory of *CW*-complexes, and the loop homotopy theory of free c. s. s. groups are equivalent ([9], [5]). While c. s. s. complexes are completely combinatorial, a considerable advantage of *CW*- complexes is the fact that a given homotopy type can often be represented by a very small model. For instance an n-sphere may be represented by a *CW*-complex with two cells (one in dimension 0 and one in dimension n), while any c. s. s. complex satisfying the extension condition of the same homotopy type contains infinitely many non-degenerate simplices in all dimensions $\geqq n$. Of course the n-sphere may be represented by a c. s. s. complex which does not satisfy the extension condition containing only two non-degenerate simplices (in the dimension 0 and n), but it can readily be seen that for a two cell *CW*-n-sphere with an $(n+1)$-cell attached by a map of degree q this (i. e. representing it by a c. s. s. complex with three non-degenerate simplices in dimensions 0, n and $n+1$) cannot be done for q sufficiently large.

Free c. s. s. groups are a fortiori c. s. s. complexes (which even satisfy the extension condition). However, as was remarked in [8], Remark 5. 6, they also very much behave like *CW*-complexes. Like a *CW*-complex which is determined by its cells and their attaching maps, a free c. s. s. group is determined (see § 2) by a suitable subset (the elements of which are called generators) together with an attaching element for every generator.

It is the purpose of this note to show that this similarity is not accidental, but that for every *CW*-complex K (with only one 0-cell) one may construct a free c. s. s. group B which has the loop homotopy type of the loop space on K and which has as many generators in dimension $n-1$ as K has cells in dimension n, and conversely. This implies that for any homotopy type equally small models exists among free c. s. s. groups as among *CW*-complexes. For instance if K is the above two cell *CW*-n-sphere with an $(n+1)$-cell attached

* Received July 15, 1958.

by a map of degree q, then the free c. s. s. group which has a generator α in dimension $n-1$ and a generator β in dimension n with attaching element α^q has the loop homotopy of the loop space on K.

There are two chapters and an appendix. Chapter I contains several propositions which illustrate the similarity of CW-complexes and free c. s. s. groups, while Chapter II deals with the exact relationship between them. In the Appendix, which is more or less independent of the rest of the paper, we consider the operations union, cone and suspension and their analogues for c. s. s. groups.

Free use will be made of the notation and the results of [4] and [5].

Chapter I. Similarity of CW-complexes and free c. s. s. groups.

2. CW-bases. The CW-behaviour of free c. s. s. groups can easiest be described using a special kind of bases, therefore called CW-bases. We recall the definition and the main properties.

Definition 2.1. Let F be a free c. s. s. group ([5], Definition 5.1). A subset $\mathfrak{F} \subset F$ will be called a *CW-basis* of F if

(a) $\mathfrak{F}_n = \mathfrak{F} \cap F_n$ freely generates F_n for all $n \geqq 0$,

(b) $\mathfrak{F}$ is closed under degeneracies, i. e. $\sigma \in \mathfrak{F}_n$ implies $\sigma\eta^i \in \mathfrak{F}_{n+1}$ for all $0 \leqq i \leqq n$,

(c) if $\sigma \in \mathfrak{F}_n$ is non-degenerate, then $\sigma\epsilon^i = e_{n-1}$ ($e_{n-1} =$ unit of F_{n-1}) for all $0 \leqq i < n$.

The non-degenerate elements of $\mathfrak{F}$ are called *generators*; for a generator $\sigma \in \mathfrak{F}_n$ the elements $\sigma\epsilon^n \in F_{n-1}$ will be called the *attaching element* of σ.

The following proposition was proved in [8], § 5.

PROPOSITION 2. 2. *Every free c. s. s. group has a CW-basis.*

It is easily seen that a free c. s. s. group has more than one CW-basis. In going from one CW-basis to another, Propositions 2. 5 and 2. 6 below will be useful. In order to formulate them we need:

Notational convention 2. 3. Let F be a c. s. s. group and let $\mathfrak{F} \subset F$ be a set which is closed under degeneracies (Definition 2. 1(b)). For every non-degenerate element $\sigma \in \mathfrak{F} \cap F_n$ we will then denote by $\{\mathfrak{F} - \sigma\}$ the set obtained from $\mathfrak{F}$ by omitting σ and all its degeneracies; and if $\tau \in F_n, \not\subset \mathfrak{F}$

is non-degenerate, then $\{\mathfrak{F}+\tau\}$ will denote the set obtained from $\mathfrak{F}$ by adding τ and all its degeneracies.

Definition 2.4. For every integer $n \geqq 0$, the *n-skeleton* F^n of a c. s. s. group F is the c. s. s. subgroup $F^n \subset F$ generated by F_n, i. e. the smallest c. s. s. subgroup containing F_n. By the (-1)*-skeleton* F^{-1} we mean the c. s. s. subgroup generated by the element e_0.

PROPOSITION 2.5. *Let $\mathfrak{F}$ be a CW-basis of the free c. s. s. group F. If $\sigma \in \mathfrak{F}_n$ is a generator and $\tau \in F_n$ is in subgroup generated by $\mathfrak{F}_n - \sigma$ and is such that $\tau\epsilon^i = e_{n-1}$ for $0 \leqq i < n$, then $\{\mathfrak{F} - \sigma + \sigma\tau\}$ is a CW-basis of F.*

The proof of this proposition is straightforward.

An immediate consequence is:

PROPOSITION 2.6. *If $\sigma \in \mathfrak{F}_n$ is a generator and $\tau \in (F^{n-1})_n$ is such that $\tau\epsilon^i = e_{n-1}$ for $0 \leqq i < n$, then $\{\mathfrak{F} - \sigma + \sigma\tau\}$ is a CW-basis of F.*

3. Some similarities. It is clear from the definition of a CW-basis that a free c. s. s. group is completely determined by the generators of a CW-basis together with their attaching elements, just as CW-complexes ([13]) are determined by their cells and attaching maps. This analogy may be carried further. If to a CW-complex a cell is attached by two different attaching maps, which are homotopic, then the resulting complexes have the same homotopy type. A slightly stronger result holds for free c. s. s. groups: attaching a generator by two different attaching elements which are homotopic in the sense of [4], § 2, yields free c. s. s. groups which are not only of the same homotopy type, but are even isomorphic. For the exact formulation we need:

Definition 3.1. Let K be a CW-complex, $L \subset K$ a subcomplex, c a cell of $K - L$ and λ its attaching map. Then K is said to be *obtained from L by attaching c by the attaching map λ*, if $K = L \cup c$ (Notation $K = L \cup_\lambda c$ or $K = L \cup c$).

Definition 3.2. Let F be a free c. s. s. group, $A \subset F$ a c. s. s. subgroup and $\sigma \in F_n - A_n$ a non-degenerate n-simplex. Then F is said to be *obtained from A by attaching σ by attaching element $\alpha = \sigma\epsilon^n$* if there exists a CW-basis $\mathfrak{A}$ of A such that $\{\mathfrak{A} + \sigma\}$ is a CW-basis of F (Notation $F = A *_\alpha \sigma$ or $F = A * \sigma$). It is an immediate consequence of Proposition 2.5 that if one CW-basis $\mathfrak{A}$ of A is such that $\{\mathfrak{A} + \sigma\}$ is a CW-basis of F, then every CW-basis of A has this property.

PROPOSITION 3.3. *Let* $K = L \cup_\lambda c$ *and* $M = N \cup_\nu d$, *where* $\dim c = \dim d$, *and let* $f\colon L \to N$ *be a homeomorphism such that* $f \circ \lambda \sim \nu$. *Then* f *may be extended to a homotopy equivalence* $f'\colon K \to M$.

This well known proposition follows immediately from the definition of a CW-complex ([13]. We now state its analogue.

PROPOSITION 3.4. *Let* $F = A *_\alpha \sigma$ *and* $G = B *_\beta \tau$, *where* $\dim \sigma = \dim \tau = n$, *let* $h\colon A \to B$ *be an isomorphism and let* $\rho \in B_n$ *be such that* $\rho\colon h\alpha \sim \beta$ ([4], *Definition* 2.2). *Then* h *may be extended to an isomorphism* $h'\colon F \to G$ *such that* $h'\sigma = \tau \cdot \rho^{-1} \cdot \rho\epsilon^{n-1}\eta^{n-1}$.

Proof. The definition of the relation $\sim$ ([4], § 2) implies that

$$(\rho^{-1} \cdot \rho\epsilon^{n-1}\eta^{n-1})\epsilon^i = e_{n-1}, \qquad 0 \leqq i < n,$$

$$(\rho^{-1} \cdot \rho\epsilon^{n-1}\eta^{n-1})\epsilon^n = \beta^{-1} \cdot h\alpha$$

and hence in view of Definition 3.2 and the freeness of F there exists exactly one c.s.s. homomorphism $h'\colon F \to G$ such that $h' \mid A = h$ and

$$h'\sigma = \tau \cdot \rho^{-1} \cdot \rho\epsilon^{n-1}\eta^{n-1}.$$

Let $\mathfrak{A}$ be a CW-basis of A, then $\mathfrak{F} = \{\mathfrak{A} + \sigma\}$ is a CW-basis of F. Furthermore $\{h\mathfrak{A} + \tau\}$ is a CW-basis of G and in view of Proposition 2.5 so is $\mathfrak{G} = \{h\mathfrak{A} + \tau \cdot \rho^{-1} \cdot \rho\epsilon^{n-1}\eta^{n-1}\}$. That h' is an isomorphism now follows from the fact that h' induces a one to one correspondence between the elements of $\mathfrak{F}$ and those of $\mathfrak{G}$.

Another "well known" proposition on CW-complexes and its analogue for free c.s.s. groups are:

PROPOSITION 3.5. *Let* $K = L \cup_\lambda c$ *and* $M = N \cup_\nu d$, *where* $\dim c = \dim d$, *and let* $f\colon L \to N$ *be a homotopy equivalence such that* $f \circ \lambda = \nu$. *Then the map* $f'\colon K \to M$ *given by* $f' \mid L = f$ *and* $f' \circ \sigma_c = \sigma_d$ (*where* σ_c *and* σ_d *denote the characteristic maps of* c *and* d) *is a homotopy equivalence.*

PROPOSITION 3.6. *Let* $F = A *_\alpha \sigma$ *and* $G = B *_\beta \tau$, *where* $\dim \sigma = \dim \tau$, *and let* $h\colon A \to B$ *be a loop homotopy equivalence* ([5], §§ 3, 4) *such that* $h\alpha = \beta$. *Then the c.s.s. homomorphism* $h'\colon F \to G$ *given by* $h' \mid A = h$ *and* $h'\sigma = \tau$ *is a loop homotopy equivalence.*

Proof of Proposition 3.5. Let C denote the mapping cylinder of f ([3], p. 108), let $l\colon L \to C$ and $n\colon N \to C$ be the injections and $p\colon C \to N$ the projection and denote by

$$l'\colon K \to C \cup_{l \circ \lambda} c', \qquad p'\colon C \cup_{l \circ \lambda} c' \to M$$

$$n'\colon M \to C \cup_{n \circ \nu} d', \qquad p''\colon C \cup_{n \circ \nu} d' \to M$$

the continuous maps such that

$$\begin{array}{ll} l' \mid L = l & l' \circ \sigma_c = \sigma_{c'} \\ n' \mid N = n & n' \circ \sigma_d = \sigma_{d'} \\ p' \mid C = p & p' \circ \sigma_{c'} = \sigma_d \\ p'' \mid C = p & p'' \circ \sigma_{d'} = \sigma_d \end{array}$$

where σ_c denotes the characteristic map of c, etc. Because $l(L)$ and $n(N)$ are strong deformation retracts of C ([3]), it follows readily that l' and n' are homotopy equivalences. Clearly p'' is a homotopy inverse of n' and hence p'' is also a homotopy equivalence. By Proposition 3.3 the identity map $i\colon C \to C$ may be extended to a homotopy equivalence $i'\colon C \cup c' \to C \cup d'$ and it is readily seen that i' may be chosen in such a manner that $p' \sim p'' \circ i'$. Hence p' is a homotopy equivalence and the proposition now follows from the fact that $f' = p' \circ l'$.

Proof of Proposition 3.6. The proof of Proposition 3.6 is completely analogous to that of Proposition 3.5, using loop homotopy ([5], §§ 3, 4) instead of homotopy and Proposition 3.4 instead of Proposition 3.3; the analogue of the mapping cylinder is the free c. s. s. group obtained from $(I \otimes A) * B$ by identifying for every simplex $\sigma \in A$

$$(\epsilon_1{}^0 \eta^0 \cdots \eta^{(\dim \sigma)-1} \otimes \sigma) \text{ with } h\sigma.$$

The details are left to the reader.

Chapter II. Relation between *CW*-complexes and free c. s. s. groups.

4. Twisting functions. In relating a CW-complex and a free c. s. s. group we need the following two intermediate notions.

(a) The first Eilenberg subcomplex of the total singular complex of a topological space with base point ([1]).

(b) J. C. Moore's notion of a twisting function, relating a c. s. s. complex and a c. s. s. group ([11]).

We briefly recall the definition of the latter and give some of its properties.

Definition 4.1. Let S be a *reduced* c. s. s. complex (i. e. S has only one 0-simplex) and let B be a c. s. s group. A *twisting function* $t\colon S \to B$ then is a function which lowers dimension by one and is such that for every integer $n > 0$ and every simplex $\sigma \in S_n$

$$
\begin{aligned}
(t\sigma)\epsilon^i &= t(\sigma\epsilon^i) && 0 \leqq i < n-1,\\
(t\sigma)\epsilon^{n-1} &= t(\sigma\epsilon^{n-1}) \cdot (t(\sigma\epsilon^n)^{-1}) &&\\
(t\sigma)\eta^i &= t(\sigma\eta^i) && 0 \leqq i \leqq n-1,\\
e_n &= t(\sigma\eta^n). &&
\end{aligned}
$$

The notion of a twisting function is closely related with the construction G of [4], which assigns to a reduced c. s. s. complex S a free c. s. s. group GS which has the homotopy type of the loops on S. We recall its definition: For every integer $n \geqq 0$, G_nS is a group which has

(i) one generator $\bar{\sigma}$ for every $(n+1)$-simplex $\sigma \in S_{n+1}$,

(ii) one relation $\overline{\tau\eta^n} = e_n$ for every n-simplex $\tau \in S_n$.

The face and degeneracy homomorphism are given by

$$
\begin{aligned}
\bar{\sigma}\epsilon^i &= \overline{\sigma\epsilon^i} && 0 \leqq i < n\\
\bar{\sigma}\epsilon^n &= \overline{\sigma\epsilon^n} \cdot (\overline{\sigma\epsilon^{n+1}})^{-1} &&\\
\bar{\sigma}\eta^i &= \overline{\sigma\eta^i} && 0 \leqq i \leqq n.
\end{aligned}
$$

The following propositions express the close relationship between the construction G and twisting functions. Their proofs are straightforward.

PROPOSITION 4.2. *Let S be a reduced c. s. s. complex, let B be a c. s. s. group and let $t\colon S \to B$ be a twisting function. Then there exists one c. s. s. homomorphism $gt\colon GS \to B$ such that for every simplex $\sigma \in S$*

$$(gt)\bar{\sigma} = t\sigma$$

PROPOSITION 4.3. *The function g of Proposition 4.2 sets up a one to one correspondence between*

(a) *the twisting functions $S \to B$,*

(b) *the c. s. s. homomorphisms $GS \to B$.*

With a twisting function $t\colon S \to B$ one may associate ([11], [4]) a principal fibre bundle with S as base and B as fibre. If the total complex of

this bundle is contractible then following J. W. Milnor ([10], [4]) we call B a *loop complex* of S (under t). This notion of being a loop complex may also be defined using the construction G instead of twisting functions. For the case that B is free this is done in the following proposition.

PROPOSITION 4.4. *Let S be a reduced c.s.s. complex, let B be a free c.s.s. group and let t: $t: S \rightarrow B$ be a twisting function. Then B is a loop complex complex of S under t ([4], Definition 6.3) if and only if the map $gt: GS \rightarrow B$ is a loop homotopy equivalence.*

The proof of this proposition is similar to that of [5], Theorem 11.2.

5. The main relation. In this section we shall define a relation between CW-complexes with one 0-cell and free c.s.s. groups and state its main properties. In order to simplify the argument only CW-complexes of which the characteristic maps of a special kind (called reduced CW-complexes) will be considered.

Let Δ_n denote an Euclidean n-simplex with vertices $A_0, \cdots, A_n$ and let $\Lambda_{n-1} \subset \Delta_n$ be the union of all its faces except the one opposite A_{n-1}. Then we define

Definition 5.1. A CW-complex K will be called *reduced* if

(a) K contains only one 0-cell p,

(b) for every integer $n > 0$ and every n-cell $c \in K$, the characteristic map is a map $\sigma_c: \Delta_n \rightarrow K$ such that $\sigma_c(\Lambda_{n-1}) = p$.

Definition 5.2. Let K be a reduced CW-complex, p its only 0-cell, and denote by $S(K)$ the first Eilenberg subcomplex of its total singular complex ([1]), i.e. an n-simplex of $S(K)$ is any continuous map $\sigma: \Delta_n \rightarrow K$ such that $\sigma(A_i) = p$ for all i. Let B be a free c.s.s. group and let $t: S(K) \rightarrow B$ be a twisting function (Definition 4.1). Then we will say that t is *regular* if

(a) the elements $t\sigma_c$ (where c runs through the cells of $K - p$) are distinct and form the generators of a CW-basis of B,

(b) for every subcomplex $L \subset K$,

$$t(S(L)) \subset B(L),$$

where $B(L) \subset B$ denotes the c.s.s. subgroup generated ([4], § 5) by the elements $t\sigma_c$ for which $c \in L$.

An immediate consequence of this definition is:

PROPOSITION 5.3. *If* $t: S(K) \to B$ *is regular, then so is* $t \mid S(L): S(L) \to B(L)$ *for every subcomplex* $L \subset K$ *and in particular* $t \mid S(K^n): S(K^n) \to B^{n-1}$ *for all* $n \geqq 0$.

The following example is a rather trivial one; in several proofs it will, however, be used as a starting point for induction.

Example 5.4. Let K consist of one point, let B have only one element in every dimension and let $t: S(K) \to B$ be the only such twisting function. Then clearly t is regular. Moreover the unique map $gt: GS(K) \to B$ (§ 4) is an isomorphism.

The main properties of regular twisting functions may be summed up in the following theorems.

THEOREM 5.5. *If* $t: S(K) \to B$ *is regular, then* B *is a loop complex of* $S(K)$ *under* t (§ 4 *and* [4], § 6). *I.e. there exists a principal bundle with basis* $S(K)$, *fibre* B, *twisting function* t *and a contractible total complex.*

COROLLARY 5.6. *If* $t: S(K) \to B$ *is regular, then for every subcomplex* $L \subset K$, $B(L)$ *is a loop complex of* $S(L)$ *under* $t \mid S(L)$; *in particular* B^{n-1} *is a loop complex of* $S(K^n)$ *under* $t \mid S(K^n)$ *for all* $n \geqq 0$.

COROLLARY 5.7. *Let* ϕ *be the only* 0*-simplex of* $S(K)$. *Then the boundary homomorphisms*

$$\partial^n: \pi_i(S(K^n); \phi) \to \pi_{i-1}(B^{n-1}; e_0)$$

of the fibre sequence associated with the principal bundle

$$((S(K^n); \phi), B^{n-1}, t \mid S(K^n))$$

([4], §§ 3, 6), *are isomorphisms for all* i *and* n.

Proof of Theorem 5.5. It suffices (Proposition 4.4) to show that the map $gt: GS(K) \to B$ is a loop homotopy equivalence. This is done by induction on the cells of K.

Order the cells of K in such a manner that $\dim c < \dim d$ implies $c < d$ and denote by $L_c \subset K$ the subcomplex consisting of all cells d with $d < c$. Let $K_c = L_c \cup c$ and suppose it has already been shown that $g(t \mid S(K_d))$ is a loop homotopy equivalence for $d < c$; then clearly $g(t \mid S(L_c))$ is so. Let $Q \subset S(K_c)$ be the subcomplex consisting of $S(L_c)$ and the simplex σ_c and its degeneracies and let $j: Q \to S(K_c)$ be the inclusion map. Then (Proposition 3.6) the composition $g(t \mid S(K_c)) \circ Gj: GQ \to B(K_c)$ is a loop homotopy equivalence. The natural map $p(L_c): |S(L_c)| \to L_c$ of the geo-

metric realization of $S(L_c)$ onto L_c is a homotopy equivalence ([9]) and so is (Proposition 3.5) the composition $p(K_c) \circ |j| : |Q| \to K_c$. As $p(K_c)$ is also a homotopy equivalence, it follows that j is a weak homotopy equivalence. [5], § 11 now yields that Gj is a loop homotopy equivalence and hence so is $g(t \mid S(K_c))$. This proves the induction step.

In order to be able to start the induction we must show that $g(t \mid S(K^0)) : GS(K^0) \to B^{-1}$ is a loop homotopy equivalence. This is example 5.4.

That gt is a loop homotopy equivalence now follows by induction.

THEOREM 5.8. *Let $t: S(K) \to B$ be regular and let $\mathfrak{B}$ denote the CW-basis of B consisting of the elements $t\sigma_c$ and their degeneracies. Then*

(a) *t induces a one to one correspondence between the cells of K and the geneartors of $\mathfrak{B}$ one dimension lower,*

(b) *for every integer $n > 0$ and every n-cell $c \in K$ we have*

$$\partial^{n-1}\alpha_c = \beta_c,$$

where $\alpha_c \in \pi_{n-1}(S(K^{n-1}); \phi)$ denotes the element containing the attaching map of the cell c and $\beta_c \in \pi_{n-2}(B^{n-2}; e_0)$ is the element containing the attaching element $(t\sigma_c)\epsilon^{n-1}$ of the corresponding generator $t\sigma_c$ of $\mathfrak{B}$.

Proof. Part (a) is a restatement of definition 5.2(a), while part (b) follows immediately from the facts that the attaching map of c is homotopic with $\sigma_c\epsilon^{n-1}$ and that $t(\sigma_c\epsilon^{n-1}) = (t\sigma_c)\epsilon^{n-1}$ and from the definition of the boundary homomorphism ∂^{n-1} ([4], § 3).

Remark 5.9. The definition of a regular twisting function could be slightly weakened by replacing condition 5.2(b) by

(b′) $$t(S(K^n)) \subset B^{n-1} \text{ for all } n \geqq 0.$$

In this case the second half of Proposition 5.3, Theorem 5.5, the second half of Corollary 5.7 and Theorem 5.8 remain true.

6. Existence theorems. It will be shown that every reduced CW-complex is related to a free c. s. s. group by a regular twisting function and conversely. In order to prove this we need the following theorem which shows how, starting from a CW-complex and free c. s. s. group which are related, one may obtain another such pair.

THEOREM 6.1. *Let $K = L \cup_\lambda c$ be a reduced CW-complex and let $B = C *_\alpha \sigma$ be a free c.s.s. group, where* $\dim c = 1 + \dim \sigma = n$. *Let*

s: $S(L) \to C$ be a regular twisting function and suppose that $\partial^{n-1}\{\lambda\} = \{\alpha\}$, i. e. there exists an element $\rho \in C_{n-1}$ such that ρ: $s(\sigma_c \epsilon^{n-1}) \sim \alpha$ ([4], Definition 2. 2). Then there exists a twisting function t: $S(K) \to B$ such that

(a) *t is regular,*

(b) *$t \mid S(L) = s$,*

(c) *$t\sigma_c = \sigma \cdot \rho^{-1} \cdot \rho \epsilon^{n-2} \eta^{n-2}$.*

Proof. Let $Q \subset S(K)$ be the subcomplex consisting of $S(L)$ and σ_c and its degeneracies. Then (see the proof of Theorem 5. 5) the inclusion map j: $Q \to S(K)$ induces a loop homotopy equivalence Gj: $GQ \to GS(K)$. Similarly for every subcomplex $M \subset K$ the intersection $Gj \cap GS(M)$: $GQ \cap GS(M) \to GS(M)$ is a loop homotopy equivalence and iterated application of the loop homotopy extension theorem ([7], § 6) yields the existence of a loop homotopy inverse h: $GS(K) \to GQ$ of Gj such that

(i) $h \mid GQ$ is the identity,

(ii) $h(GS(M)) \subset GS(M)$ for every subcomplex $M \subset K$.

As ρ: $s(\sigma_c \epsilon^{n-1}) \sim \alpha$ it follows by application of Propositions 3. 4 and 3. 6 that the map gs: $GS(L) \to C$ may be extended to a loop homotopy equivalence k: $GQ \to B$ such that $k\bar{\sigma}_c = \sigma \cdot \rho^{-1} \cdot \rho \epsilon^{n-2} \eta^{n-2}$. Let t: $GS(K) \to B$ be the unique twisting function (Proposition 4. 3) such that $gt = k \circ h$. A straightforward computation then yields that t has all the desired properties.

THEOREM 6. 2. *For every reduced CW-complex K there exist a free c. s. s. group B and a regular twisting function t: $S(K) \to B$.*

The proof of Theorem 6. 2 is similar to that of Theorem 6. 3; induction is used on the cells of K as in the proof of Theorem 5. 5. The details are left to the reader.

THEOREM 6. 3. *For every free c. s. s. group B there exist a reduced CW-complex K and a regular twisting function t: $S(K) \to B$.*

Proof. Let $\mathfrak{B}$ be a CW-basis of B. The proof then goes by induction on the generators of $\mathfrak{B}$. Order the generators of $\mathfrak{B}$ in such a manner that $\dim \sigma < \dim \tau$ implies $\sigma < \tau$, let $C_\sigma \subset B$ be the c. s. s. subgroup generated by the generators τ for which $\tau < \sigma$ and let $B_\sigma = C_\sigma * \sigma$. Suppose for all $\tau < \sigma$ a reduced CW-complex K_τ and a regular twisting function t_τ: $S(K_\tau) \to B_\tau$ have already been defined such that for $\tau < \rho < \sigma$, K_τ is a subcomplex of K_ρ and $t_\tau = t_\rho \mid S(K_\tau)$. Let $L_\sigma = \bigcup_{\tau < \sigma} K_\tau$ and $s_\sigma = \bigcup_{\tau < \sigma} t_\sigma$; then clearly s_σ:

$S(L_\sigma) \to C_\sigma$ is regular. If $B_\sigma = C_\sigma *_\alpha \sigma$, $\dim \sigma = n - 1$, define K_σ by $K_\sigma = L_\sigma \cup_\lambda . c$, i.e. by attaching a cell c to L_σ, where $\dim c = n$ and its attaching map λ is such that $\partial^{n-1}\{\lambda\} = \{\alpha\}$. This is possible in view of Corollary 5.7. Theorem 6.1 now yields an extension $t_\sigma : S(K_\sigma) \to B_\sigma$ of s_σ which is regular. This proves the induction step. The theorem now follows by induction starting from Example 5.4.

7. Homotopy uniqueness theorems. The question in how far a related CW-complex and free c.s.s. group determine each other will be answered in Theorems 7.1 and 7.2 below. Two CW-complexes related to the same free c.s.s. group are clearly of the same homotopy type, but the other way around a slightly stronger statement may be made: two free c.s.s. groups related to the same CW-complex are not only of the same loop homotopy type, but are even isomorphic.

We now give the exact formulation.

THEOREM 7.1. *Let $t : S(K) \to B$ and $s : S(L) \to C$ be regular twisting functions. Then for every continuous map $f : K \to L$ there exist c.s.s. homomorphisms $a : B \to C$ such that diagram 7.1a is commutative up to a loop homotopy; any two such maps are loop homotopic. And for every c.s.s. map $a : B \to C$ there exist continuous maps $f : K \to L$ such that diagram 7.1a is commutative up to a loop homotopy; any two such maps are homotopic.*

7.1a
$$\begin{array}{ccc} GS(K) & \xrightarrow{GS(f)} & GS(L) \\ \downarrow{\scriptstyle gt} & & \downarrow{\scriptstyle gs} \\ B & \xrightarrow{a} & C \end{array}$$

THEOREM 7.2. *Let $t : S(K) \to B$ and $s : S(K) \to C$ be regular twisting functions. Then there exist isomorphisms $f : B \to C$ such that diagram 7.2a is commutative up to a loop homotopy. Any two such isomorphisms are loop homotopic.*

(7.2a)
$$\begin{tikzcd} & GS(K) \arrow[dl, "gt"'] \arrow[dr, "gs"] & \\ B \arrow[rr, "f"] & & C \end{tikzcd}$$

Remark 7.3. If the definition of a regular twisting function is weakened as in Remark 5.9, then Theorems 6.1, 6.2, 6.3, 7.1 and 7.2 remain true.

Proof of Theorem 7.1. The second half of the theorem follows immediately from the fact that gs and gt are loop homotopy equivalences (Proposition 4.4 and Theorem 5.5), while the first half is a consequence of [5], §§ 9 and 11.

For the proof of Theorem 7.2 we need:

PROPOSITION 7.4. *Let $t\colon S(K)\to B$ and $s\colon S(K)\to C$ be regular, let $K=L\cup c$ and let $f(L)\colon B(L)\to C(L)$ be an isomorphism such that the following diagram is commutative up to a loop homotopy*

$$\begin{tikzcd} & GS(L) \arrow[dl, "g(t\,|\,S(L))"'] \arrow[dr, "g(s\,|\,S(L))"] & \\ B(L) \arrow[rr, "f(L)"] & & C(L) \end{tikzcd} \tag{7.4a}$$

Then $f(L)$ may be extended to an isomorphism $f\colon B\to C$ such that diagram 7.2a *is commutative up to a loop homotopy.*

Proof of Theorem 7.2. The second half of the theorem follows immediately from the fact that gs and gt are loop homotopy equivalences (Proposition 4.4 and Theorem 5.5). The proof of the first half goes by induction on the cells of K as in the proof of Theorem 5.5, starting from Example 5.4.

For every cell $c\in K$ let K_c, $L_c\subset K$ be as in the proof of Theorem 5.5 and suppose that for every cell $e<c$ an isomorphism $f(K_e)\colon B(K_e)\to C(K_e)$ has already been defined such that diagram 7.4a, with K_e instead of L, is commutative up to a loop homotopy and such that for $e<d<c$, $f(K_e) = f(K_d)\,|\,B(K_e)$. Let $f(L_c)=\bigcup_{e<c} f(K_e)$ then clearly $f(L_c)\colon B(L_c)\to C(L_c)$ is an isomorphism such that diagram 7.4a, with L_c instead of L, is commutative up to a loop homotopy. Proposition 7.4 yields an extension $f(K_c)$ of $f(L_c)$ which is an isomorphism and is such that diagram 7.4a, with K_c instead of L, is commutative up to a loop homology, which proves the induction step.

Proof of Proposition 7.4. Let $Q\subset S(K)$ be as in the proof of Theorem 6.1. Then the injection $Gj\colon GQ\to GS(K)$ is a loop homotopy equivalence and hence it suffices to show that $f(L)$ may be extended to an isomorphism $f\colon B\to C$ such that the following diagram is commutative up to a loop homotopy.

$$\begin{tikzcd} & GQ \arrow[dl, "g(t \mid Q)"'] \arrow[dr, "g(s \mid Q)"] & \\ B \arrow[rr, "f"] & & C \end{tikzcd}$$

Let $h(L) : I \otimes GS(L) \to C(L)$ be a loop homotopy

$$h(L) : g(s \mid S(L)) \sim (f(L) \circ g(t \mid S(L))),$$

then by the loop homotopy extension theorem ([7], § 6) $h(L)$ may be extended to a loop homotopy $h \colon g(s \mid Q) \sim k$. A straightforward computation, using Proposition 2.5, shows that h may be chosen such that $C = C(L) * k\bar{\sigma}_c$. As $B = B(L) * t\sigma_c$ and

$$f(L)((t\sigma_c)\epsilon^{n-1}) = f(L)(t(\sigma_c\epsilon^{n-1})) = (f(L) \circ gt)\bar{\sigma}_c\epsilon^{n-1} = k(\bar{\sigma}_c\epsilon^{n-1})$$

it follows (Proposition 3.4) that $f(L)$ admits an extension to an isomorphism $f \colon B \to C$ such that $f(t\sigma_c) = k\bar{\sigma}_c$. The proposition now follows from the fact that $k = f \circ g(t \mid Q)$ and $k \sim g(s \mid Q)$.

Appendix.

8. Union and free product. It will be shown (Theorems 8.1 and 8.3) that the free product of two c. s. s. groups is the analogue of the notion of union, with the base points identified, for CW-complxes or c. s. s. complexes.

For two reduced CW-complexes K and K' let $K \vee K'$ denote their union with identification of the 0-cels and let $B * B'$ denote the free product of the c. s. s. groups B and B'. Then we have

THEOREM 8.1. *For any two regular twisting functions $t \colon S(K) \to B$ and $t' \colon S(K') \to B'$, there exists a regular twisting function*

$$s \colon S(K \vee K') \to B * B'.$$

Proof. This follows immediately from Theorem 6.1 using induction on the cells of K or on those of K'.

For two reduced c. s. s. complexes S and S' let $S \vee S'$ denote their union with identification of the 0-simplices and their degeneracies. Then ([4], Corollary 20.2)

THEOREM 8.2. *If S and S' are reduced c. s. s. complexes, then*

$$G(S \vee S') = GS * GS'$$

The analogue of Theorem 8.1 for c. s. s. complexes then is:

THEOREM 8.3. *Let the free c.s.s. groups B and B' be loop complexes* ([4], § 6) *of the reduced c.s.s. complexes S and S' under the twisting functions t and t' respectively. Then $B * B'$ is a loop complex of $S \vee S'$ under the twisting function $t''\colon S \vee S' \to B * B'$ given by*

$$t''\sigma = t\sigma, \qquad \sigma \in S, \qquad\qquad t''\sigma = t'\sigma, \qquad \sigma \in S'.$$

Proof. By Proposition 4.4 gt and gt' are loop homotopy equivalences, and so is ([6], Theorem 5.3) the map $gt * gt'\colon GS * GE' \to B * B'$. The theorem now follows from Theorem 8.2, Proposition 4.4 and the fact that $gt'' = gt * gt'$.

9. The cone. A construction C will be described which assigns to a free c. s. s. group B a free c. s. s. group CB and it will be shown that this construction is the analogue of the reduced cone constructions for CW-complexes and c. s. s. complexes. This construction resembles the construction W of Eilenberg-MacLane ([12]); it uses free products instead of dircet products.

Definition 9.1. The *cone* CB of a c. s. s. group B is the c. s. s. group defined as follows. For every integer $n \geqq 0$

$$C_nB = B_n * B_{n-1} * \cdots * B_0.$$

For every integer $k \geqq 0$ and every element $\sigma \in B_n$ let $(k,\sigma) \in C_{n+k}B$ denote the image of σ under the injection $B_n \to C_{n+k}B$. The face and degeneracy homomorphisms $\epsilon^i\colon C_nB \to C_{n-1}B$ and $\eta^i\colon C_n \to C_{n+1}B$ then are given by the formulas

$$\text{(9.1a)} \qquad \begin{aligned} &(k,\sigma)\epsilon^i = (k,\sigma\epsilon^{i-k}), \qquad (k,\sigma)\eta^i = (k,\sigma\eta^{i-k}), \qquad && i \geqq k \\ &(k,\sigma)\epsilon^i = (k-1,\sigma), \qquad (k,\sigma)\eta^i = (k+1,\sigma), \qquad && i < k. \end{aligned}$$

Similarly for a c. s. s. homomorphism $f\colon B \to B'$ we define a c. s. s. homomorphism $Cf\colon CB \to CB'$ by

$$Cf(k,\sigma) = (k, f\sigma)$$

PROPOSITION 9.2. *If B is a free c.s.s. group, then so is CB.*

Proof. Let $\mathfrak{B}$ be a basis of B ([8], Definition 2.1) and let $\mathfrak{A} \subset CB$ consist of the elements $(0,\sigma)$ and $(1,\sigma)$ and their degeneracies, where σ runs through the generators of $\mathfrak{B}$. It then follows easily from Definition 9.1 that $\mathfrak{A}$ is a basis of CB.

For a reduced CW-complex K denote by CK the *reduced cone* of K, i.e. the complex obtained from $I \times K$ by shrinking to a point of the subcomplex $(1 \times K) \cup (I \times K^0)$. CK may of course be supposed to be reduced. Then we have

THEOREM 9.3. *For every regular twisting function $t\colon S(K) \to B$ there exists a regular twisting function $t'\colon S(CK) \to CB$.*

This is proved by induction on the cells of CK, using Theorem 6.1. The details are left to the reader.

We recall a definition of reduced cone for c.s.s. complexes

Definition 9.4. Let S be a reduced c.s.s. complex and ϕ its only 0-simplex. The *reduced cone* of S is the c.s.s. complex CS defined as follows. For every integer $n \geqq 0$ the n-simplices of CS are the pairs (k, σ), where $k \geqq 0$ is an integer and $\sigma \in S_{n-k}$ is a simplex, identifying $(k, \phi\eta^0 \cdots \eta^{n-k-1})$ with (n, ϕ). The face and degeneracy operators are determined by the formulas 9.1a.

A simple computation yields

THEOREM 9.5. *Let S be a reduced c.s.s. complex. Then the c.s.s. homomorphism $h\colon GCS \to CGS$ given by*

$$h(\overline{k, \sigma}) = (k, \bar{\sigma}) \qquad \sigma \in S,$$

is an isomorphism.

And of course we have

THEOREM 9.6. *For every c.s.s. group B, CB is contractible.*

Proof. The formulas 9.1a imply that the function $d\colon CB \to CB$ given by $d(k, \sigma) = (k+1, \sigma)$ is a contracting homotopy, i.e. $(d\tau)\epsilon^i = d(\tau\epsilon^{i-1})$ for $i > 0$ and $(d\tau)\epsilon^0 = \tau$. From this it readily follows that CB is contractible.

10. The suspension. By "collapsing" the cone construction C of 9.1 new construction $\bar{C}$ may be obtained which is the analogue of the reduced suspension. This construction resembles the $\bar{W}$-construction of Eilenberg-MacLane ([12]).

Definition 10.1. The *suspension* $\bar{C}B$ of a c.s.s. group B is the c.s.s. group obtained from CB by adding for every integer $n \geqq 0$ and every simplex $\sigma \in B_n$ a relation $(0, \sigma) = e_n$. This clearly implies

$$\bar{C}_n B = B_{n-1} * B_{n-2} * \cdots * B_0$$

For a c. s. s. homomorphism $f\colon B \to B'$, $\bar{C}f\colon \bar{C}B \to \bar{C}B'$ will denote the c. s. s. homomorphism induced by $Cf\colon CB \to CB'$.

PROPOSITION 10.2. *If B is a free c. s. s. group, then so is $\bar{C}B$.*

The proof is similar to that of Proposition 9.2.

For a reduced CW-complex K denote by $\bar{C}K$ the *reduced suspension* of K, i. e. the complex obtained from $I \times K$ by shrinking to a point the subcomplex $(0 \times K) \cup (1 \times K) \cup (I \times K^0)$. $\bar{C}K$ may of course be supposed to be reduced. Then

THEOREM 10.3. *For every regular twisting function $t\colon S(K) \to B$ there exists a regular twisting function $t'\colon S(\bar{C}K) \to \bar{C}B$.*

This is proved by induction on the cells of $\bar{C}K$, using Theorem 6.1. The details are left to the reader.

We recall a definition of reduced suspension for c. s. s. complexes. The definition differs from the one given in [4], § 22; the first face and degeneracy operators play a special role instead of the last (see remark at the end of [4], § 1).

Definition 10.4. Let S be a reduced c. s. s. complex and ϕ its only 0-simplex. The *reduced suspension* of S is the c. s. s. complex $\bar{C}S$ obtained from the reduced cone CS (Definition 9.4) by identifying for every integer $n > 0$ and every simplex $\sigma \in S_n$

$$(0, \sigma) \text{ with } (n, \phi)$$

An immediate consequence of Theorem 9.5 then is

THEOREM 10.5. *Let S be a reduced c. s. s. complex. Then the c. s. s. homomorphism $\bar{h}\colon G\bar{C}S \to \bar{C}GS$ given by*

$$\bar{h}(\overline{k, \sigma}) = (k, \bar{\sigma})$$

is an isomorphism.

Finally we have

THEOREM 10.6. *Let the free c. s. s. group B be a loop complex of the reduced c. s. s. complex S under a twisting function t. Then $\bar{C}B$ is a loop complex of $\bar{C}S$.*

Proof. It follows from Proposition 4.4 that $gt\colon GS \to B$ is a loop homotopy equivalence and from Theorem 9.6 that $C(gt)\colon CGS \to CB$ is so. Consequently ([7], Theorem 5.3) their abelianizations $gt/[gt, gt]$ and

$C(gt)/[C(gt), C(gt)]$ are homotopy equivalences. Let $j: B \to CB$ be the c. s. s. monomorphism given by $j\sigma = (0, \sigma)$ for all $\sigma \in B$. Then

$$(CB/[CB, CB])/(j(B)/[j(B), j(B)]) \approx \bar{C}B/[\bar{C}B, \bar{C}B].$$

A similar relation holds for GS and it follows by application of the five lemmas ([2,], p. 16) that $\bar{C}(gt)/[\bar{C}(gt), \bar{C}(gt)]$ is also a homotopy equivalence. $\bar{C}GS$ and $\bar{C}B$ are connected and hence ([6], Theorem 6.1) the map $\bar{C}(gt): \bar{C}GS \to \bar{C}B$ is a loop homotopy equivalence and the theorem now follows by application of Theorem 10.5 and Proposition 4.4.

THE HEBREW UNIVERSITY,
JERUSALEM, ISRAEL.

REFERENCES.

[1] S. Eilenberg, "Singular homology theory," *Annals of Mathematics*, vol. 45 (1944), pp. 407-447.

[2] S. Eilenberg and N. Steenrod, *Foundations of algebraic topology*, Princeton University Press (1952),

[3] P. J. Hilton, *An introduction to homotopy theory*, Cambridge University Press (1953).

[4] D. M. Kan, "A combinatorial definition of homotopy groups," *Annals of Mathematics*, vol. 67 (1958), pp. 282-312.

[5] ———, "On homotopy theory and c. s. s. groups," *Annals of Mathematics*, vol. 68 (1958), pp. 38-53.

[6] ———, "On the homotopy relations for c. s. s. maps," *Boletin de la Sociedad Matematica Mexicana* (1957), pp. 75-81.

[7] ———, "On c. s. s. categories," *Boletin de la Sociedad Matematicica Mexicana*,

[8] ———, "Minimal free c. s. s. groups," *Illinois Journal of Mathematics*, vol. 2 (1958), pp. 537-547.

[9] J. W. Milnor, "The geometric realization of a semi-simplical complex," *Annals of Mathematics*, vol. 65 (1957), pp. 357-362.

[10] ———, "The construction *FK*," Princeton University (1956) (mimeographed).

[11] J. C. Moore, "Semi-simplical complexes and Postnikov systems," *Proceedings of the International Symposium on Algebraic Topology and its Applications*, Mexico, 1956.

[12] ———, "Construction sur des complexes d'anneaux," Seminaire H. Cartan (1954/1955), no. 12.

[13] J. H. C. Whitehead, "Combinatorial homotopy I," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 213-245.

HARMONIC INTEGRALS ON FOLIATED MANIFOLDS.*

By Bruce L. Reinhart.

In the paper [5], we considered harmonic integrals on local product manifolds, that is, manifolds having two families of submanifolds in complementary dimensions, such that locally they look like the product of two euclidean spaces. The metric was assumed to be such that this local product could be taken in the sense of Riemannian manifolds. The results obtained were such as to suggest that analogous theorems could be proved if we assumed only one family of submanifolds, with a suitable choice of metric. This is indeed the case. We shall show in § 4 that on compact manifolds, the cohomology of base-like differential forms (defined in § 2) is isomorphic to the harmonic space of a certain semi-definite Laplacian (defined in § 3). The metric is assumed to be bundle-like in the sense of [6]; that paper may be referred to for examples of foliated manifolds possessing such a metric. In § 5, we discuss the meaning of our harmonic integral theorem for these examples.

1. Definitions. By a manifold M, we mean a C^∞ differentiable manifold; topologically, it is a connected, orientable, separable, locally euclidean Hausdorff space. We shall assume given on M (of dimension n) a C^∞ completely integrable q form Θ, that is, a locally decomposable, non-zero q form such that locally $d\Theta$ is a multiple of Θ [6]. A manifold with such a form will be called a foliated manifold. We shall also assume given a locally decomposable p $(=n-q)$ form Ω such that $\Omega \wedge \Theta$ is never zero. (The existence of such an Ω follows from the existence of Θ [6]. Since Ω does not occur in the final theorem, the fact that it is not unique does not matter). Given such a Θ, we can find about each point a coordinate neighborhood with coordinates $(x^1, \cdots, x^p, y^1, \cdots, y^q)$ such that

(i) $|x^i| \leqq 1$, $|y^\alpha| \leqq 1$,

(ii) The integral manifolds of Θ are given locally by $y^1 = c^1, \cdots, y^q = c^q$ for constants c^α satisfying $|c^\alpha| \leqq 1$.

* Received July 16, 1958.

(Here and hereafter, Latin indices run from 1 to p, and Greek indices from 1 to q.) Such a coordinate neighborhood will be called flat, while each of the slices given by a set of equations $y^\alpha = c^\alpha$ will be called a plaque. If U is a flat neighborhood, the quotient space of U by its plaques will be called the local base and be denoted by U_y. The natural projection $\pi\colon U \to U_y$ will be called the local projection.

Since Ω is locally decomposable, we may assume [6] that there exist in U differential forms ω^i and vectors v_α such that:

(i) $\Omega = \omega^1 \wedge \cdots \wedge \omega^p$ in U,

(ii) $\{\omega^1, \cdots, \omega^p, dy^1, \cdots, dy^q\}$ and $\{\partial/\partial x^1, \cdots, \partial/\partial x^p, v_1, \cdots, v_q\}$ are dual bases for the cotangent and tangent spaces respectively at each point of U. Hence, $\omega^i = dx^i + \sum a_\alpha{}^i dy^\alpha$ and $v_\alpha = \partial/\partial y^\alpha + \sum b_\alpha{}^i \partial/\partial dx^i$.

Throughout this paper, all local expressions for differential forms and vectors will be taken with respect to these bases.

2. Base-like cohomology. Our aim in this paragraph is to compute the special properties of the exterior derivative which hold for a foliated manifold, and to show how they may be applied to define a notion of base-like cohomology groups. These properties arise from the decomposition of differential forms into components in the following way: Any m form may be expressed locally as

$$\sum_{\substack{i_1 < \cdots < i_r \\ \alpha_1 < \cdots < \alpha_s}} \sum_{r+s=m} \phi_{i_1 \cdots i_r \alpha_1 \cdots \alpha_s}(x, y)\, \omega^{i_1} \wedge \cdots \wedge \omega^{i_r} \wedge dy^{\alpha_1} \wedge \cdots \wedge dy^{\alpha_s}.$$

We then define $\Pi_{r,s}\phi$ to be the sum of all those terms having a fixed r and s. Since under change of flat coordinate system, $\{\{dy^\alpha\}\}$ goes into $\{\{dy^{*\alpha}\}\}$ and $\{\{\omega^i\}\}$ goes into $\{\{\omega^{*i}\}\}$, this concept is independent of the choice of coordinate system. Here by $\{\{a^i\}\}$ we mean the vector space generated by the elements a^i. $\Pi_{r,s}\phi$ is called the component of type (r, s) of ϕ. (This notion is defined intrinsically in [4]). The type decomposition of differential forms induces a type decomposition of the exterior derivative d by the rule $(\Pi_{t,u}d)\phi = \sum_{r,s}\Pi_{r+t,s+u} d \Pi_{r,s}\phi$. Let $\Pi_{1,0}d = d'$ and $\Pi_{0,1}d = d''$. In general, there will be a component $\Pi_{-1,2}d$; since we are interested only in forms of type $(0, s)$, we shall not introduce a notation for this component.

Proposition 1. *If ϕ is of type $(0, s)$, then $d\phi = d'\phi + d''\phi$. Moreover, $d'\phi = 0$ if and only if ϕ depends only upon y, in the sense that locally $\phi = \sum \phi_{\alpha_1 \cdots \alpha_s}(y)\, dy^{\alpha_1} \wedge \cdots \wedge dy^{\alpha_s}$.*

Proof. Any ϕ of type $(0,s)$ has the local expression

$$\phi = \sum \phi_{\alpha_1\cdots\alpha_s}(x,y)\,dy^{\alpha_1}\wedge\cdots\wedge dy^{\alpha_s}.$$

Hence

$$d\phi = \sum(\partial\phi_{\alpha_1\cdots\alpha_s}/\partial x^i)\,\omega^i\wedge dy^{\alpha_1}\wedge\cdots\wedge dy^{\alpha_s}$$
$$+\sum(\partial\phi_{\alpha_1\cdots\alpha_s}/\partial y^\alpha - a_\alpha{}^i\,\partial\phi_{\alpha_1\cdots\alpha_s}/\partial x^i)\,dy^\alpha\wedge dy^{\alpha_1}\wedge\cdots\wedge dy^{\alpha_s}$$

where ω^i and $a_\alpha{}^i$ have the same meaning as in § 1, $\omega^i = dx^i + a_\alpha{}^i dy^\alpha$. The desired type decomposition is immediately obvious. Furthermore, $d'\phi = 0$ if and only if for every set of indices $\{\alpha_1,\cdots,\alpha_s,i\}$, $\partial\phi_{\alpha_1\cdots\alpha_s}/\partial x^i = 0$. Since we assume that all forms considered are of class C^∞, this proves the proposition.

Definition. A form of type $(0,s)$ which is annihilated by d' will be called a base-like form.

Let A'' be the vector space of global differential forms which satisfy the conditions of Proposition 1; $A'' = \sum A''^s$, where A''^s consists of forms of type $(0,s)$. Restricted to A'', $d''^2 = d^2 = 0$, so we may consider the cohomology of A'' under d''. Call the groups H''^s so defined the base-like cohomology groups of M. We shall show that in the situation of a bundle-like metric on a compact manifold, these groups are finite dimensional and satisfy the usual duality relations.

Given any orientable differentiable manifold, we can always choose coordinate systems so that the Jacobians of the coordinate changes in overlapping neighborhoods are identically equal to 1. A generalization of this fact is essential in what follows.

PROPOSITION 2. *Given any foliated manifold covered by flat neighborhoods U_ν with coordinates $(x_\nu{}^1,\cdots,x_\nu{}^p,y_\nu{}^1,\cdots,y_\nu{}^q)$, we can rechoose coordinates so that the partial Jacobians $J_{\nu\mu} = (\partial x_\nu{}^i/\partial x_\mu{}^j)$ are identically 1, provided that they are all positive.*

Proof. Consider the sheaf of germs of positive real valued functions, defined by exponentiating the sheaf of germs of real valued functions. This is a fine sheaf since the exponential map is an isomorphism. $\{J_{\nu\mu}\}$ is a 1-cocycle with coefficients in this sheaf; hence, we can choose functions J_ν in U_ν such that $J_{\nu\mu} = J_\mu/J_\nu$. Introduce new coordinates by the formulas:

$$X_\nu{}^1 = \int_0^{x_\nu} J_\nu(t,x_\nu{}^2,\cdots,x_\nu{}^p,y_\nu{}^1,\cdots,y_\nu{}^q)\,dt,$$
$$X_\nu{}^i = x_\nu{}^i,\qquad i = 2,\cdots,p,$$

$$Y_\nu^\alpha = y_\nu^\alpha, \qquad \alpha = 1, \cdots, q.$$

Then $(\partial X_\nu^i/\partial X_\mu^j = J_\nu \cdot J_{\nu\mu} \cdot 1/J_\mu \equiv 1.$

3. The Laplacian for base-like forms. We wish to define a Laplacian operator which will map the set of base-like forms into itself; this may be thought of as a Laplacian in the variables y. For this to be possible, we need to assume the existence of a bundle-like metric.

Definition. A Riemannian metric is bundle-like if and only if it is representable in each flat neighborhood by an expression of the form

$$ds^2 = \sum g_{ij}(x,y)\omega^i\omega^j + \sum g_{\alpha\beta}(y)\, dy^\alpha dy^\beta.$$

In this definition, the essential restriction is that on the coefficients $g_{\alpha\beta}$; if these were allowed to depend on all variables, a metric could always be found satisfying the definition [5].

The tensor $\sum g_{\alpha\beta}(y)\, dy^\alpha dy^\beta$ defines a duality operation on the base-like forms by the formula

$$(*''\phi)_{\alpha_1\cdots\alpha_{q-s}} = \sum_{\beta_1<\cdots<\beta_s} \delta^{1\cdots q}{}_{\beta_1\cdots\beta_s\alpha_1\cdots\alpha_{q-s}} (\det(g_{\alpha\beta}))^{\frac{1}{2}} g^{\beta_1\nu_1}\cdots g^{\beta_s\nu_s}\phi_{\nu_1\cdots\nu_s}$$

Then, in analogy with the ordinary case, we define

$$\delta''\phi = (-1)^{qs+q+1} *'' d'' *'' \phi$$

where ϕ is a base-like form of degree s, and

$$\Delta'' = d''\delta'' + \delta'' d''.$$

We wish to introduce a measure on M in such a way that Δ'' is self-adjoint in the Hilbert space of square integrable base-like forms. For this, Proposition 2 is the chief tool. Let $dV'' = (\det(g_{\alpha\beta}))^{\frac{1}{2}} dy^1 \wedge \cdots \wedge dy^q$ be the base-like volume element. In the coordinate neighborhood U_ν, we may consider the form $dx_\nu^1 \wedge \cdots \wedge dx_\nu^p$. Under coordinate changes, if we choose the neighborhoods as in Proposition 2, this goes into $dx_\mu^1 \wedge \cdots \wedge dx_\mu^p +$ terms involving the dy_μ^α. Taking the exterior product with dV'', the latter terms drop out and we find that $dV = dV'' \wedge dx^1 \wedge \cdots \wedge dx^p$ is a well-defined differential form giving a volume element on M. This in turn defines an inner product on base-like forms by the formula

$$(\phi, \psi) = \int_M \phi \wedge *''\psi \wedge dx^1 \wedge \cdots \wedge dx^p.$$

We next need to derive the formulas covering adjointness on a compact manifold. For this purpose, we recall that d'' restricted to base-like forms is the same as d restricted to base-like forms. Hence, for ϕ a base-like form and ψ a base-like s form, both of C^∞, we have

$$0=\int_M d(\phi\wedge *''\psi\wedge dx^1\cdots dx^p)=\int_M d''(\phi\wedge *''\psi)\wedge dx^1\wedge\cdots\wedge dx^p$$
$$=\int_M d''\phi\wedge *''\psi\wedge dx^1\wedge\cdots\wedge dx^p-\int_M \phi\wedge *''\delta''\psi\wedge dx^1\wedge\cdots\wedge dx^p,$$

which means $(d''\phi,\psi)=(\phi,\delta''\psi)$ for all base-like forms of arbitrary degree. It is clear that then $(\Delta''\phi,\psi)=(\phi,\Delta''\psi)$ for all base-like forms. If we complete in the given norm to get a Hilbert space, then the technique of Gaffney [2] enables us to show that if we take the closures of d'' and δ'' and denote them by the same symbols, then $\Delta''=d''\delta''+\delta''d''$ is a positive self-adjoint operator.

4. Green's operator. In this paragraph, we shall assume that M is compact and show how the techniques of [5] can be modified to show the existence on the Hilbert space of base-like differential forms of a bounded self-adjoint operator G'' such the $\Delta''G''\phi=\phi-H''\phi$ and $G''H''\phi=0$, where H'' is the projection of ϕ onto the kernel of the closed operator Δ''. The concept of coherent sheaf introduced there is not needed here; we merely restrict our attention to base-like forms. All symbols $'$ of that paper become $''$ here, and the role of the variables x and y is interchanged. In the paper [5], much use is made of the fact that a torsionless almost product metric induces a product measure on local product neighborhoods; moreover, these neighborhoods may be chosen with orthonormal coordinates. In this paper, we use instead a finite covering of M by neighborhoods such that the Jacobian in x is identically 1. At any point, we can choose a subneighborhood of one of the given neighborhoods which is orthonormal in y and has all $y^\alpha=0$ at the given point; this can be done without changing the variables x. Then the form dV'' induces a product measure on each such neighborhood, and the subneighborhoods may be used in the proof of the (purely local) differentiability lemma, the only place where the orthonormal coordinate system is used [5, Theorem 6.2]. We thus derive the main theorem of this paper. Because of the restriction in Proposition 2, we need the concept of orientable foliation.

Definition. A foliation will be said to be orientable if a covering by flat

coordinate neighborhoods can be chosen so that $(\partial x_\nu{}^i/\partial x_\mu{}^j) > 0$ in each intersection of two of them.

THEOREM. *Let M be a compact manifold with orientable foliation and bundle-like metric. Then there is defined on the Hilbert space of base-like forms on M a bounded symmetric operator G'' such that*

$$\Delta'' G''\phi = G''\Delta''\phi = \phi - H''\phi,$$
$$G''H''\phi = H''G''\phi = 0,$$
$$d''G''\phi = G''d''\phi, \qquad \delta''G''\phi = G''\delta''\phi.$$

Moreover, the kernel of Δ'' is finite dimensional.

Proof. The theorem is proved by the techniques used in proving Theorem 6.3 and Lemma 6.4 of [5], including therefore all the preceding parts of § 6. The modifications mentioned above are understood to be made throughout.

Let $b^s(y)$ be the dimension of the cohomology group of base-like forms of degree s on M.

COROLLARY. *$b^s(y)$ is finite, and $b^s(y) = b^{q-s}(y)$.*

Proof. This follows by standard techniques. Indeed, $d''\phi = 0$ implies that $\phi = d''\delta''G''\phi + H''\phi$, so is cohomologous to its harmonic part. If $H''\phi = d''\psi$, then $(H''\phi, H''\phi) = (H''\phi, d''\psi) = (\delta''H''\phi, \psi) = 0$; hence each cohomology class contains just one harmonic form. Thus, the cohomology groups are additively isomorphic to the kernel of Δ''. The finiteness of $b^s(y)$ follows immediately, while the equation $*''H''\phi = H''*''\phi$ implies the desired duality property.

5. Examples.

We shall conclude the paper by showing how the theory just developed applies to some examples of foliated manifolds with bundle-like metrics. For notation, and proof that these examples satisfy the definition, see [6].

The first case to be considered is that of a fibre space (M, π, B). Here M is foliated by the subsets $\pi^{-1}(b)$ for $b \in B$; assume these fibres are connected.

PROPOSITION 3. *ϕ is base-like on M if and only if $\phi = \pi^*(\phi_0)$ for some ϕ_0 on B, where π^* is the map on differential forms induced by the projection π.*

Proof. Suppose first that $\phi = \pi^*(\phi_0)$, where ϕ_0 is an s form. By the local triviality, we see that ϕ must be of type $(0, s)$. Moreover, its value is independent of the point along a given fibre; hence, locally the coefficients

depend only upon y. Conversely, let $f\colon U \to M$ be a local cross-section, where U is a contractible euclidean neighborhood in B. Then $\phi_0 = f^*(\phi \mid f(U))$ is a form on U independent of f. Moreover, it clearly has the property that $\pi^*(\phi_0) = \phi$. ϕ_0 is clearly independent of the choice of flat coordinate system in M and corresponding coordinate system in B. This proves the proposition.

Interpreting the theorem for the case of fibre spaces, we see that it is essentially nothing but the usual Hodges' theorem for B; the only difference lies in that all computations may be carried out in M without referring to B explicitly.

The next example of interest is that of the foliation of M by orbits of a group of isometries H, under the assumption that all of these orbits are of the same dimension. If X is an element of the Lie algebra of H, it induces a vector field X_* on M which is everywhere tangent to the orbits of H; in fact, the set of all X_* generates the tangent space to the orbit thropgh each point. Let $i(X_*)$ denote the operation of contraction by X_*. Then Koszul [3] has defined the notion of *forme basique*; it is a differential form on M which satisfies the two conditions:

(i) $i(X_*)(\phi) = 0$ for all X in the Lie algebra of H.

(ii) $h_*(\phi) = \phi$ for all $h \in H$.

PROPOSITION 4. *Let the connected Lie-group H act on M as a group f isometries with all orbits of the same dimension. Then ϕ is base-like if d only if* (i) *and* (ii) *hold.*

Proof. Suppose (i) and (ii) hold, and look at ϕ in a flat coordinate system. Since $\{X_*\}$ generates the same space as $\{\partial/x^i\}$, (i) implies that ϕ is expressible in terms of dy alone. By (ii), its value is independent of the point on the orbit, that is, of x. Thus, ϕ is base-like. Conversely, if ϕ is base-like, it clearly satisfies (i). Moreover, for h near the identity, (ii) may be proved by looking at a local coordinate system. To prove it for distant h, join them by a path, which may be covered by a finite number of translates of a suitable neighborhood of the identity. Since H is connected, the theorem is proved.

As our example, consider the unit tangent bundle M to a V-manifold B with isolated singularities; this is a sort of singular fibre space, in which the fibres are spheres except over the singular points, where they are spherical space forms. Let $(U_\alpha, G_\alpha, \eta_\alpha)$ be a local uniformizing structure in B; then a differential form ψ on $\bar{U}_\alpha = \eta_\alpha(U_\alpha)$ is defined as a form on U which is invariant by G_α. It is clear that $\pi^*(\psi)$, defined on $\pi^{-1}(\bar{U}_\alpha)$, is base-like

(by the same argument as in Proposition 3) and invariant by G_α. The proof of Proposition 3 may then be generalized to prove the following

PROPOSITION 5. *Let M be the unit tangent bundle of the V-manifold B with isolated singularities. Then the base-like forms of M are precisely those induced from B by the projection mapping.*

It follows, just as in the fibre space case, that Hodge's theorem holds for B. This is a special case of the theorem of Baily [1] for arbitrary compact V-manifolds.

UNIVERSITY OF CHICAGO.

REFERENCES.

[1] W. L. Baily, Jr., "The decomposition theorem for V-manifolds," *American Journal of Mathematics*, vol. 78 (1956), pp. 862-888.

[2] M. P. Gaffney, "Hilbert space methods in the theory of harmonic integrals," *Transactions of the American Mathematical Society*, vol. 78 (1955), pp. 426-444.

[3] J. L. Koszul, "Sur certaines groupes de transformation de Lie," *Colloque de géométrie différentielle* (Strasbourg), Paris, Centre National de Recherche Scientifique, 1953.

[4] H. K. Nickerson and D. C. Spencer, *Differentiable manifolds and sheaves*, notes, Princeton University, 1955.

[5] B. L. Reinhart, "Harmonic integrals on almost product manifolds," *Transactions of the American Mathematical Society*, vol. 88 (1958), pp. 243-276.

[6] ———, "Foliated manifolds with bundle-like metric," *Annals of Mathematics* (2), vol. 69 (1959), pp. 119-132.

ON THE INDEPENDENCE OF THE AXIOM OF CONSTRUCTIBILITY.* [1]

By J. R. SHOENFIELD.

IN [2], Gödel has shown that the Axiom of Choice and the Generalized Continuum Hypothesis are conseqences of a more general axiom. This axiom, which we call the Axiom of Constructibility, states that every set is constructible (in the notation of [2], $V=L$).

It is natural to ask if the Axiom of Constructibility follows from the Axiom of Choice and the Generalized Continuum Hypothesis. A difficulty in answering this question is that the independence of the Axiom of Constructibility from the axioms of set theory (i. e., the axioms A—D of [2]) has not been settled. This suggests we try to prove the following relative independence statement: if the Axiom of Constructibility is not provable from axioms A—D, then it is not provable from axioms A—D, the Axiom of Choice, and the Generalized Continuum Hypothesis.

The object of this paper is to prove two results which are slightly weaker than the statement just mentioned.[2] We first introduce weakened forms of the Generalized Continuum Hypothesis and the Axiom of Constructibility.

GCH′: *There is an ordinal* α_0 *such that* $2^{\aleph_\alpha}=\aleph_{\alpha+1}$ *for* $\alpha \geqq \alpha_0$.

ACon′: *Every set of integers is constructible.*

THEOREM 1. *If the Axiom of Constructibility is not provable from axioms* A—D, *then it is not provable from axioms* A—D, *the Axiom of Choice, and GCH′.*

THEOREM 2. *If ACon′ is not provable from axioms* A—C, *then it is*

* Received March 17, 1958.

[1] Presented to the Summer Institute of Symbolic Logic in 1957 at Cornell University. This research was supported by a National Science Foundation fellowship.

[2] The possibility of proving Theorem 2 by the methods of this article was noted some time ago by Gödel.

The results of this article have been obtained independently by Lévy. More recently, Lévy has obtained extensions of these results, which will be published soon.

not provable from axioms A—D, the Axiom of Choice, and the Generalized Continuum Hypothesis (and hence the Axiom of Constructibility is not provable from these axioms).

We now give the proof of Theorem 1. Assume the hypothesis of the theorem. Then axioms A—D and the axiom $V \neq L$ form a consistent set. From axiom D and $V \neq L$, it follows that there is a set $x \in V - L$ such that $x \cap (V - L) = 0$, i.e., such that $x \subset L$. Hence it is consistent with axioms A—D to introduce a new individual constant 'a' and the axioms:

$$\mathfrak{M}(a) \tag{1}$$

$$a \notin L \tag{2}$$

$$a \subset L. \tag{3}$$

We now introduce the set operations $\mathfrak{F}_1$—$\mathfrak{F}_8$ of 9.1 (all decimal references are to [2]), and a ninth operation:

$$\mathfrak{F}_9(XY) = a \cap X.$$

We then introduce all the definitions of Chapter V of [2], with $\mathfrak{F}_1$—$\mathfrak{F}_8$ replaced by $\mathfrak{F}_1$—$\mathfrak{F}_9$. (In particular, we replace '9' by '10' in 9.2 and 9.21.) We designate the so defined concepts by the symbols used in [2] followed by an asterisk; e.g., L^*, constructible*.

Now we introduce a model Δ^* as follows: class is interpreted as constructible* class; set is interpreted as constructible* set; membership is interpreted as membership; and a is interpreted as a.

The results of Chapters 5-7 of [2] hold also for the model Δ^*. For the only place in which the operations $\mathfrak{F}_1$—$\mathfrak{F}_8$ are considered individually is in the proof of 9.5; and this is easily extended to include $\mathfrak{F}_9$, since $\mathfrak{F}_9(xy) \subset x$. Hence we obtain: Δ^* is a model for axioms A—D, and L is absolute*.

If we relativize the theorem $L \subset V$ to the model Δ^*, we obtain $L \subset L^*$. Hence by (3), $a \subset L^*$. By the analogue of 9.63, it follows that $a \subset x$ for some $x \in L^*$. Since $a = \mathfrak{F}_9(x, x)$, we have $a \in L^*$, which is the relativization of (1) to Δ^*. Since (2) and (3) are absolute*, Δ^* is a model for (1)-(3). Noting that $\mathfrak{F}_9$ is absolute*, we prove as in Chapter 7 of [2] that L^* is absolute*, and hence that the relativization of $V = L^*$ to Δ^* is $L^* = L^*$. Hence Δ^* is a model for $V = L^*$. This proves:

Lemma. *If $V = L$ is not provable from axioms A—D, the axioms A—D, (1)-(3), and $V = L^*$ are consistent.*

Theorem 1 will follow from the lemma if we show A—D, (1)-(3), and $V = L^*$ imply the Axiom of Choice and GCH′. For the Axiom of Choice, this is immediate (see [2], page 53). To prove GCH′, choose α_0 so that the order* of every element of a is $< \aleph_{\alpha_0}$. We then proceed as in Chapter VIII of [2]. The proofs of 12.4, 12.5, and 12.51 are unchanged. We modify 12.6 by adding the hypothesis that m and m' include $\aleph_{\alpha_0}$. In the proof of 12.6, it is necessary to add a further case to the cases on page 60. The result needed is:

$$F^{*}\text{‘}\alpha \in a \cap F^{*}\text{‘}\beta \equiv F^{*}\text{‘}\alpha' \in a \cap F^{*}\text{‘}\beta'.$$

In view of the induction hypothesis I, this will follow from:

$$F^{*}\text{‘}\alpha \in a \equiv F^{*}\text{‘}\alpha' \in a.$$

By symmetry, it is sufficient to show that $F^{*}\text{‘}\alpha \in a$ implies $F^{*}\text{‘}\alpha' \in a$. Let γ be the order* of $F^{*}\text{‘}\alpha$. Then $\gamma < \aleph_{\alpha_0}$. Since m and m' include $\aleph_{\alpha_0}$ and G is an order isomorphism, $\gamma' = \gamma$. Hence, using induction hypothesis II and noting $\gamma \leqq \alpha < \eta$, we have $F^{*}\text{‘}\alpha = F^{*}\text{‘}\gamma = F^{*}\text{‘}\gamma' = F^{*}\text{‘}\alpha'$; whence $F^{*}\text{‘}\alpha' \in a$.

We then prove as in [2] that 12.6 implies 12.3, provided that in 12.3 we require m and o to include $\aleph_{\alpha_0}$. This form of 12.3 implies 12.2 whenever $\alpha \geqq \alpha_0$. For in the proof of 12.2 from 12.3, m is chosen so that $\omega_{\alpha_0} \subset \omega_\alpha \subset m$; and o is an ordinal such that $\overline{\overline{o}} = \omega_\alpha$, so that $\omega_{\alpha_0} \subset \omega_\alpha \subset o$. Finally, 12.2 for $\alpha \geqq \alpha_0$ implies GCH′ as in [2]. This completes the proof of Theorem 1.

Theorem 2 is proved similarly. We first observe that axiom D is not required in the consistency proof of [2]. (The uses of axiom D in proving M1 on page 10 are easily eliminated. The development of ordinals without use of axiom D is explained, e.g., in [3]).

We now proceed as in the proof of Theorem 1. From the consistency of the negation of ACon′ with A—D, we obtain the consistency of (1), (2), and:

(3′) $$a \subset \omega.$$

Clearly (3′) implies (3). In the proof of the lemma, we need only make the additional observation that (3′) is absolute*. (This is proved by the methods of Chapter VII of [2].) In the last part of the proof, we need only observe that we may take $\alpha_0 = 0$; for, as is easily proved, the order* of every integer is finite.

It remains to prove $V = L^*$ implies axiom D. Let A be a non-empty

constructible* class, and let x be the element of A having the smallest order*. Then $\mathfrak{Ex}(x, A)$ by 9.5.

We note that axiom D apparently cannot be omitted from the hypothesis of Theorem 1. For since axiom D is known to be independent of axioms $A - C$ ([1]), and since $V = L$ implies axiom D (as above), $V = L$ is independent of axioms $A - C$.

INSTITUTE FOR ADVANCED STUDY
AND
DUKE UNIVERSITY.

REFERENCES.

[1] P. Bernays, "A system of axiomatic set theory, Part VII," *Journal of Symbolic Logic*, vol. 19 (1954), pp. 81-96.

[2] K. Gödel, *The Consistency of the Continuum Hypothesis*, Princeton University Press, 1940.

[3] J. C. Shepherdson, "Inner models for set theory, Part I," *Journal of Symbolic Logic*, vol. 16 (1951), pp. 161-190.

IMAGES OF PLANE CONTINUA.*

By M. K. Fort, Jr.[1]

1. Introduction. A *continuum* is a compact, connected, metric space. We define K to be the continuum which consists of all points in the plane having polar coordinates (r, θ) for which $r = 1$, $r = 2$, or $r = (2 + e^{\theta})/(1 + e^{\theta})$.

The following two theorems are the main results obtained in this paper.

THEOREM 1. *A plane continuum which does not separate the plane cannot be mapped continuously onto K.*

THEOREM 2. *A plane continuum cannot be mapped continuously onto the dyadic solenoid.*

The second of these theorems generalizes the known theorem which states that the dyadic solenoid cannot be imbedded in a plane.

Our two theorems give information pertinent to the following questions, whose answers are not known, and which seem to be of interest to topologists.[2]

Question 1. Is there a continuum which can be mapped continuously onto every other continuum?

Question 2. Is there a plane continuum which can be mapped continuously onto every other plane continuum?

Question 3. What characterizes all continuous images of a pseudo-arc?

Question 4. What characterizes all plane continuous images if a pseudo-arc?

It follows from these theorems that:

(i) if the continuum sought in Question 1 exists, it cannot be a plane continuum;

* Received June 27, 1958.

[1] This research was partially supported by National Science Foundation Research Grant NSF-G3016.

[2] Questions 1 and 2 were raised by R. H. Bing during a recent conversation with the author. Question 3 is stated in [1], p. 72.

(ii) if the continuum sought in Question 2 exists, it must separate the plane; and

(iii) not every plane continuum is the continuous image of the pseudo-arc.

2. Proof of Theorem 1. The following lemma concerning locally trivial fiber spaces (see [1], p. 111, and [2]) is used both in the proof of Theorem 1 and in the proof of Theorem 2.

LEMMA. *Let (E,B,p) be a locally trivial fiber space such that for each $b \in B$, the fibre $p^{-1}(b)$ is totally disconnected. If f is a mapping of a connected space A into E such that pf is homotopic to a constant, then $f[A]$ is contained in a single arc component of E.*

Proof. Let $h: A \times I \to B$ be a homotopy such that $h(x,0) = pf(x)$ and $h(x,1) = b$ for some $b \in B$ and each $x \in A$. Because of the covering homotopy property, there is a homotopy $g: A \times I \to E$ such that $g(x,0) = f(x)$ and $pg = h$. Now $g \mid A \times \{1\}$ is a mapping of a connected space into the totally disconnected set $p^{-1}(b)$. It follows that there exists $q \in p^{-1}(b)$ such that $g(x,1) = q$ for all $x \in A$. Now let (x,t) be any point of $A \times I$. The mapping g takes the segment $\{(x,s) \mid t \leqq s \leqq 1\}$ into a locally connected continuum containing q, and hence $g(x,t)$ belongs to the same arc component of E as q. It follows that $f[A]$ is contained in the same arc component of E as q.

Proof of Theorem 1. We let S_1 be the unit circle in the plane, and define $p: K \to S_1$ by $p(r,\theta) = (1,\theta)$. It is easy to verify that (K, S_1, p) is a locally trivial fiber space with totally disconnected fibers.

Now, if A is a plane continuum which does not separate the plane, and f is a mapping of A into K, then pf is a mapping of a continuum which does not separate the plane into S_1. It is known (see [3], p. 93) that pf is homotopic to a constant. It follows from our lemma that $f[A]$ is contained in a single arc component of K. Our theorem now follows at once from the fact that K has three arc components.

3. Continuous roots of mappings. The proof which we give for Theorem 2 makes use of some results concerning continuous roots of mappings. We prove the facts which are needed in this section.

The unit circle S_1 is considered as the multiplicative group of complex numbers of unit modulus. If $f: A \to S_1$ is a mapping (i.e. continuous function), then a mapping $g: A \to S_1$ is a *continuous k-th root of f, k* a positive

integer, if $g(x)^k = f(x)$ for all $x \in A$. We say that f *has property D* if f has continuous 2^n-th roots for every positive integer n.

RESULT 1. *If f is homotopic to a constant, then f has property D.*

Proof. It is known (see [3], p. 68) that if f is homotopic to a constant, then there exists a continuous real valued function h on the domain A of f such that $f(x) = e^{ih(x)}$ for all $x \in A$. It follows that $g_k(x) = e^{ih(x)/k}$ defines a continuous k-th root g_k of f for each positive integer k. Thus f has property D.

RESULT 2. *If A is a locally connected continuum and $f\colon A \to S_1$ has property D, then f is homotopic to a constant.*

Proof. Since f is uniformly continuous, there exists $\epsilon > 0$ such that any subset of A of diameter less than ϵ maps under f into a subset of S_1 which is contained in an arc of length less than 1. Since A is a locally connected continuum, A has property S and we may express A as the union of subcontinua $A_1, \cdots, A_k$ each having diameter less than ϵ. Let f_j be a continuous 2^j-th root of f for each positive integer j. It is easy to see that each $f_j[A_m]$ is an arc of S_1 having length less than 2^{-j}. It follows that for $2^j > k$, $f_j[A]$ is a proper subset of S_1 (in fact, an arc of length less than $k2^{-j}$). Thus, we see that for large values of j, f_j is homotopic to a constant. Since f is a power of f_j for each j, f_j is also homotopic to a constant.

RESULT 3. *If U is an open subset of the plane, A is a compact subset of U, F is a mapping on U into S_1, and f is a continuous square root of $F \mid A$, then there exists an open set V such that $A \subset V \subset U$ and an extension of f to a continuous square root of $F \mid V$.*

Proof. Choose an open set W containing A such that the closure of W is compact and is contained in U. There exists $\delta_1 > 0$ such that if x and y are in W and $|x - y| < \delta_1$, then $|F(x) - F(y)| < 1/2$. There exists $\delta_2 > 0$ such that if a and b are in A and $|a - b| < \delta_2$, then $|f(a) - f(b)| < 1/2$. Let $\delta > 0$ be chosen so that $\delta < \delta_1$, $\delta < \delta_2$, and the $(\delta/2)$-neighborhood V of A is contained in W.

Now suppose $x \in V$. We choose $a \in A$ such that $|x - a| < \delta/2$. $F(x)$ has a unique square root s which is nearest to $f(a)$. We define $g(x) = s$. It is easy to verify that $g(x)$ is independent of the particular $a \in A$ chosen, that the function g is a continuous square root of $F \mid V$, and that g is an extension of f.

RESULT 4. *If $F: A \to B$, $G: B \to S_1$ and g is a continuous square root of G, then gF is a continuous square root of GF.*

Proof. Obvious.

RESULT 5. *If f and g are mappings of a space X into S_1 and f is homotopic to g, then f has a continuous square root if and only if g does.*

Proof. Let $p(z) = z^2$ for $z \in S_1$ and apply the homotopy lifting theorem for the locally trivial fiber space (S_1, S_1, p).

RESULT 6. *Let f be a mapping of a space X into S_1, and let A be a deformation retract of X. If $f \mid A$ has a continuous square root, then so does f.*

Proof. There exists $R: X \times I \to X$ such that:

$$R(x,0) = x \text{ for all } x \in X,$$

$$R(x,1) \in A \text{ for all } x \in X, \text{ and}$$

$$R(x,1) = x \text{ for all } x \in A.$$

We define $G = fR$, and let $g_0(x) = G(x,0)$, $g_1(x) = G(x,1)$. It follows from Result 4 and the hypothesis that $f \mid A$ has a continuous square root that g_1 has a continuous square root. Therefore, by Result 5, g_0 has a continuous square root. Since $f = g_0$, we obtain the desired result.

RESULT 7. *If A is a topological annulus, $f: A \to S_1$, and f has a continuous square root on one of the boundary curves of A, then f has a continuous square root on A.*

Proof. This result is an immediate corollary of Result 6.

RESULT 8. *If C is a plane continuum and $f: C \to S_1$ has property D, then f is homomotopic to a constant.*

Proof. It is known that f is homotopic to a constant if f can be extended over the entire plane P. Any mapping of C into S_1 can be extended to a mapping of $P - A$ into S_1, where A is a finite set and is contained in the union of the bounded components of $P - C$. It follows that it is sufficient to prove that f can be extended to a mapping of $C \cup U$ into S_1 for each bounded component U of $P - C$.

Let U be a bounded component of $P - C$, and let E be an open disk whose closure is contained in U. It is known that f can be extended to a mapping g whose domain is open and contains $C \cup (U - E)$.

Since f, and hence also g, has a continuous square root on C, by Result 3

we see that g has a continuous square root ψ on some open set $V_1 \supset C$. There exists a closed topological disk F such that: $F \subset U$, the closure of E is contained in the interior of F, $F \cup V_1 \supset U$, and the boundary of F is contained in V_1. Then $F - E$ is a topological annulus, g is defined over $F - E$, and g has the continuous square root ψ on the outer boundary B of $F - E$. It follows from Result 7 that $\psi \mid B$ can be extended to a continuous square root ϕ of $g \mid (F - E)$. We can piece together ϕ and a part of ψ to obtain a continuous square root g_1 of g on $V_1 \cup (U - E)$.

We repeat the above process and obtain a continuous square root g_2 of g_1 on $V_2 \cup (U - E)$, where V_2 is open and $C \subset V_2 \subset V_1$. Continuing, we see that g has property D on the boundary B' of E. Thus, by Result 2, $g \mid B'$ is homotopic to a constant. Hence, $g \mid B'$ can be extended continuously over $B' \cup E$. We are now able to construct a continuous extension of f over $C \cup U$.

RESULT 9. *If C is the dyadic solenoid and F is a mapping of C into S_1, then F has a continuous square root.*

Proof. We represent C as an inverse limit space, $C = \varprojlim_{n} \{X_n, f_n\}$, where for each positive integer n, $X_n = S_1$, and $f_n \colon X_{n+1} \to X_n$ is defined by $f_n(z) = z^2$. we let π_n be the projection of C onto X_n for each positive integer n. The space C is metrizable, and we assume that C is metrized by the admissible metric d defined by

$$d(x,y) = \sum_{n=1}^{\infty} \mid \pi_n(x) - \pi_n(y) \mid / 2^n.$$

It is easily seen that if $u \in X_n$, then

$$\text{diameter}\, \pi_n^{-1}(u) \leqq 2^{-n}.$$

Now, for some integer k, we are going to obtain a mapping $g_k \colon X_k \to S_1$ such that $g_k \pi_k$ is homotopic to F. In order to accomplish this, we choose $\delta > 0$ such that if $B \subset C$ and diameter $B < \delta$, then diameter $F[B] < 1$. We choose k to be a positive integer for which $2^{-k} < \delta$. Since π_k^{-1} is an upper semi-continuous set-valued function and diameter $\pi_k^{-1}(u) \leqq 2^{-k}$ for each $u \in X_k$, there exists $\eta > 0$ such that if $A \subset X_k$ and diameter $A < \eta$ then diameter $\pi_k^{-1}[A] < \delta$. Next, we choose points $p_0, p_1, \cdots, p_m, p_0$ in cyclic order on X_k such that $\mid p_i - p_{i+1} \mid < \eta$ for each i. We define $g_k \colon X_k \to S_1$ such that:

$$g_k(p_i) \in F[\pi_k^{-1}(p_i)] \text{ for each } i,$$

and

$$g \text{ is "linear" on each arc } \overline{p_i p_{i+1}}.$$

For such a g_k, it follows that $|g_k\pi_k(x) - F(x)| < 1$ for all $x \in C$, and hence $g_k\pi_k$ is homotopic to F.

Now, since $\pi_k = f_k\pi_{k+1}$, we see that

$$g_k\pi_k = g_k(f_k\pi_{k+1}) = (g_kf_k)\pi_{k+1}.$$

Both g_k and f_k are mappings of S_1 into S_1, and f_k is of degree 2. Since

$$\text{degree}(g_kf_k) = (\text{degree}\, g_k)(\text{degree}\, f_k),$$

it follows that g_kf_k is of even degree and hence has a continuous square root. We now use Result 4 to see that $(g_kf_k)\pi_{k+1}$ has a continuous square root. Since $(g_kf_k)\pi_{k+1} = g_k\pi_k$ and $g_k\pi_k$ is homotopic to F, it follows from Result 5 that F has a continuous square root.

4. **Proof of Theorem 2.** We now use the results obtained in the preceding paragraph to prove Theorem 2.

Proof of Theorem 2. Let K be a plane continuum, and let G be a mapping of K into the dyadic solenoid C. We will show that $G[K]$ is contained in a single arc component of C, and hence, since C is not arcwise connected, G does not map K *onto* C.

We represent $C = \lim\limits_{\overleftarrow{n}} \{X_n, f_n\}$, as in the proof of Result 9, and we again let π_1 be the projection of C onto $S_1 = X_1$. It is easily seen that (C, S_1, π_1) is a locally trivial fiber space with totally disconnected fibers.

It follows from Result 9 that π_1 has property D. Thus, by Result 4, π_1G has property D. Since π_1G is a mapping of a plane continuum into S_1, we apply Result 8 and see that π_1G is homotopic to a constant. It now follows from our Lemma that $G[K]$ is contained in a single arc component of C.

THE UNIVERSITY OF GEORGIA.

REFERENCES.

[1] *Summary of Lectures and Seminars*, Summer Institute on Set Theoretic Topology, Madison, Wisconsin, 1955.

[2] W. Heubsch, "On the covering homotopy theorem," *Annals of Mathematics*, vol. 61 (1955), pp. 555-563.

[3] S. Eilenberg, "Topologie du plan," *Funramenta Mathematicae*, vol. 26 (1936), pp. 61-112.

REPRESENTATION OF ELLIPTIC OPERATORS IN AN ENVELOPING ALGEBRA.*

By EDWARD NELSON [1] and W. FORREST STINESPRING.[1]

Introduction. In the study of finite-dimensional representations of a Lie group G, the corresponding infinitesimal representation of the Lie algebra and its extension to the enveloping algebra have played an important role. It is reasonable, therefore, to seek aid in the study of infinite-dimensional unitary representations of G from the infinitesimal representation. Bargmann, for example, in his paper [1] finding all irreducible unitary representations of the 2×2 real unimodular group depends heavily on the infinitesimal operators. Unfortunately, the formulation of the infinitesimal representation corresponding to an infinite-dimensional representation is plagued by the fact that in general the image operators are unbounded. Gårding constructed a dense linear manifold of the representation space on which the images of the whole enveloping alegbra are naturally defined, which is invariant under these operators, and on which these operators form a homomorphic image of the enveloping algebra. The theory of Hilbert space, however, leads one to want more. It is desirable for symmetric elements of the enveloping algebra to be represented by self-adjoint operators. The same problem arises in the context of quantum mechanics. In a unitary representation corresponding to some physical particle the images of the elements of the Lie algebra of the underlying symmetry group are momenta of some sort, and certain polynomials in them have physical interpretations. It is appropriate to ask when these operators are observables; that is, when they are essentially self-adjoint, for it is self-adjoint operators that have reasonable spectral resolutions.

Unfortunately, the images of symmetric elements do not always have reasonable interpretations as self-adjoint operators. In fact, Section 5 contains a simple example of such an operator on the Gårding subspace which has no self-adjoint extension at all. I. E. Segal has shown that an operator on the Gårding subspace has a self-adjoint closure provided that it is i times

* Received July 3, 1958.

[1] National Science Foundation Fellows.

the image of an element of the Lie algebra itself [17], or it is the image of a symmetric element in the center of the enveloping algebra [18]. In this paper we establish the same result for *elliptic* elements of the enveloping algebra and for elements commuting with them. (See Section 2 for precise results.)

Section 3 establishes a connection between second order elliptic elements of the enveloping algebra and the L_1 group algebra. This is applied in Section 4 to construct a class of Lie groups, including the inhomogeneous Lorentz group, which are not CCR groups in the sense of Kaplansky [11]. This section also contains a new proof that semi-simple matrix groups are CCR groups.

1. Notations and terminology. In this paper we shall be concerned with a Lie group G, and elements of the universal enveloping algebra $\mathcal{E}$ of its right-invariant Lie algebra; for brevity, we shall refer to $\mathcal{E}$ as the right-invariant enveloping algebra of G. We denote by $L \to L^+$ the conjugate linear anti-automorphism of $\mathcal{E}$ such that $X^+ = -X$ for X in the Lie algebra. We say that an element of $\mathcal{E}$ is elliptic if it is elliptic as a partial differential operator on G. Let T be a bounded strongly continuous representation of G on a Banach space $\mathfrak{V}$. If f is in $L_1(G)$ (an unnamed measure on G will always be left-invariant Haar measure), we write $T(f)$ for the operator $\int_G f(\sigma)T(\sigma)d\sigma$, where this integral converges in the strong operator topology. By the Gårding subspace of $\mathfrak{V}$, we mean the linear manifold spanned by all vectors $T(\phi)x$, where x is in $\mathfrak{V}$ and ϕ is in the class $C_0^\infty(G)$ of all infinitely differentiable functions on G with compact support. If L is in $\mathcal{E}$, by $dT(L)$ we mean the linear operator with the Gårding subspace for its domain such that $dT(L)(T(\phi)x) = T(L\phi)x$. This is the notation of Segal in [17].

Sometimes it is reasonable to take as the domain of the operator representing L a manifold other than the Gårding subspace. For example:

(1) the well-behaved vectors (see [17]) are a good choice for domain when they are dense;

(2) if T is the regular representation of G on a homogeneous space G/H, then $C_0^\infty(G/H)$ is a natural domain;

(3) if T is the restriction to G of a representation of a larger group, then the Gårding subspace of the larger representation may occur as domain. To handle such cases, we point out the following fact, which we shall use without comment.

THEOREM 1.1. *Let T be a bounded strongly continuous representation of a Lie group G on a Banach space. Let L be an element of the right-invariant enveloping algebra of G. Let A be an operator on the representation space with a single-valued closure such that:*

(1) *A has a dense domain which is invariant under all $T(\phi)$ with ϕ in $C_0^\infty(G)$;*

(2) *$A(T(\phi)x) = T(L\phi)x$ if x is in the domain of A.*

Then the closure of A contains $dT(L)$.

Proof. Let x be any vector in the representation space. Let $x_n \to x$ with x_n in the domain of A. Then for any ϕ in $C_0^\infty(G)$,

$$A(T(\phi)x_n) = T(L\phi)x_n \to T(L\phi)x.$$

2. Elliptic elements of the enveloping algebra and elements commuting with them.

LEMMA 2.1. *Let f be an infinitely differentiable positive definite function on a Lie group G, and let K be an element of the right-invariant enveloping algebra of G. Then $(K^+Kf)(e) \geqq 0$.*

Proof. We approximate K by a right-invariant difference operator. That is to say, for each $h > 0$, we choose numbers $c_\alpha(h)$ for each α in G, so that for fixed h, $c_\alpha(h) \neq 0$ for only finitely many α, and so that for each infinitely differentiable function g,

$$(Kg)(\sigma) = \lim_{h\to 0} \sum_\alpha c_\alpha(h) g(\alpha\sigma)$$

for all σ in G. This can be done so that

$$(K^+g)(\sigma) = \lim_{h\to 0} \sum_\beta \bar{c}_\beta(h) g(\beta^{-1}\sigma)$$

and

$$(K^+Kf)(e) = \lim_{h\to 0} \sum_{\beta\alpha} \bar{c}_\beta(h) c_\alpha(h) f(\alpha\beta^{-1}).$$

By definition of positive definite function, these last sums are non-negative for exery h.

THEOREM 2.2. *Let G be a Lie group, and let U be a strongly continuous unitary representation of G. If L is an elliptic element of the right-invariant enveloping algebra of G, then the closure of $dU(L^+)$ is the adjoint of $dU(L)$.*

Proof. Case I: $L = K^+K$ for some K in the enveloping algebra. We combine two observations to get that $A = dU(L)$ is essentially self-adjoint, i. e. has a self-adjoint closure.

(1) If x is in the Gårding subspace, $(Ax, x) \geqq 0$. For $A = dU(K^+K) = dU(K^+)dU(K)$, so that $(Ax, x) = (dU(K)x,\, dU(K)x) \geqq 0$ when x is in the Gårding subspace.

(2) $A + 1$ has a dense range. For suppose x is orthogonal to the range of $A + 1$. Then $((A+1)U(\phi)x, x) = 0$ for all ϕ in $C_0^\infty(G)$. Rewriting yields $\int ((L+1)\phi)(\sigma)(U(\sigma)x, x)\,d\sigma = 0$; in other words, the function $(U(\cdot)x, x)$ is a weak solution of the partial differential equation $(L+1)f = 0$. Since $L + 1$ is elliptic, $(U(\cdot)x, x)$ is, in fact, analytic (see, for example, [10]), and $(L+1)(U(\cdot)x, x) = 0$ in the ordinary pointwise sense. But this contradicts Lemma 1, which shows that $[L(U(\cdot)x, x)](e) \geqq 0$.

These two observations imply that A is essentially self-adjoint, because they show that $(A+1)^{-1}$ is bounded and densely defined.

Case II: L is a general elliptic element. From Case I we deduce that $dU(L^+L) = dU(L^+)dU(L)$ is essentially self-adjoint. But this fact implies that the closure of $dU(L^+)$ is the adjoint of $dU(L)$ according to the following lemma.

LEMMA 2.3. *Let $\mathfrak{D}$ be a dense linear manifold in a Hilbert space $\mathfrak{H}$. Let T and T' be linear transformations whose domains are $\mathfrak{D}$ and whose ranges are contained in $\mathfrak{D}$ such that T' is contained in the adjoint of T. If $T'T$ is essentially self-adjoint, then the closure of T' is the adjoint of T.*

Proof. We must show that the graph of T^* contains no non-zero element orthogonal to the graph of T'. Suppose $\{a, b\}$ is an element of the graph of T^* that is orthogonal to the graph of T'. In other words, $b = T^*a$, but $(y, a) + (T'y, b) = 0$ for all y in $\mathfrak{D}$. If x is in $\mathfrak{D}$, then Tx is in $\mathfrak{D}$, and hence $(Tx, a) + (T'Tx, b) = 0$; that is, $(x, b) + (T'Tx, b) = 0$. But $1 + T'T$ has a dense range. Consequently $b = 0$. So $(y, a) = 0$ for all y in $\mathfrak{D}$; and, therefore, $a = 0$.

COROLLARY 2.4. *Let G be a Lie group, and let U be a strongly continuous unitary representation of G. Let L be an elliptic element of the right-invariant enveloping algebra $\mathcal{E}$ of G such that $L^+ = L$. If M is any element of $\mathcal{E}$ such that $dU(M^+M)$ commutes with $dU(L)$, then the closure of $dU(M^+)$ is the adjoint of $dU(M)$.*

Proof. Let r be an integer greater than the order of M, $A = dU(L^{2r})$, $B = dU(M^+M)$ and $C = A + B$. Then A and C represent elliptic operators, and so are essentially self-adjoint by Theorem 2.2. The operators A and C commute on the Gårding subspace, but we need the stronger fact that their closures $\bar{A}$ and $\bar{C}$ commute, i.e. have commuting spectral resolutions. To see this, notice that the bounded operators $(1+A)^{-1}(1+C)^{-1}$ and $(1+C)^{-1}(1+A)^{-1}$ agree on their common domain, the range of $(1+A)(1+C) = (1+C)(1+A)$. But $(1+A)(1+C)$ represents an elliptic operator, and so is essentially self-adjoint by Theorem 2.2, and thus has a dense range (by the positivity of $A + C + AC$). Consequently $\bar{A}$ and $\bar{C}$ commute.

Let $B_1 = \bar{A} - \bar{C}$. This is essentially self-adjoint, by the spectral theorem. If we show that B_1 is contained in $\bar{B}$, then the corollary will follow, by Lemma 2.3. Let x be in the domain of B_1. Then x is in the domain of $\bar{C}$, so there is a sequence $\{x_n\}$ in the Gårding subspace such that $x_n \to x$ and $Cx_n \to \bar{C}x$. Now for all y in the Gårding subspace, $\| Ay \| \leqq \| Cy \|$, since

$$(Cy, Cy) = (Ay, Ay) + (By, By) + 2(BdU(L^r)y, dU(L^r)y)$$

by the commutativity of $dU(L)$ and $dU(M^+M)$, and all three terms are positive. In particular this is true for $y = x_n - x_m$, so that for the same sequence $\{x_n\}$ we also have $Ax_n \to \bar{A}x$, and so $Bx_n \to B_1x$. That is, B_1 is contained in the closure of B, concluding the proof.

As examples to Corollary 2.4, notice that if G is Abelian or compact then the enveloping algebra $\mathcal{E}$ contains a central symmetric elliptic element, so that for every M in $\mathcal{E}$ the closure of $dU(M^+)$ is the adjoint of $dU(M)$, as is well-known. Also if G is aribtrary but M is central, then M commutes with a symmetric elliptic element, and the same conclusion follows, yielding a result of Segal [18]. If G is semi-simple with maximal essential compact subgroup K, then the Casimir operator on G is of the form $-\Delta_1 + \Delta_2$, where Δ_1 is a central elliptic element of the enveloping algebra of K and $\Delta_1 + \Delta_2$ is elliptic on G. Any M in the enveloping algebra of G which commutes with Δ_1 also commutes with $\Delta_1 + \Delta_2$ since $-\Delta_1 + \Delta_2$ is central, and therefore the closure of $dU(M^+)$ is the adjoint of $dU(M)$.

By Theorem 1.1, all of the above examples persist on the Gårding subspace of a representation of a larger group containing G. In particular, if X is in the Lie algebra of a Lie group and p is any real polynomial, then $dU(p(iX))$ is essentialy self-adjoint since $p(iX)$ is in the enveloping algebra of the one-parameter (Abelian) subgroup generated by X. For iX itself this was established by Segal [17].

3. Second order elliptic operators. In this section some additional information is derived in the second order case using the maximum principle. This will be applied in the following section.

THEOREM 3.1. *Let G be a Lie group, let $X_1,\cdots,X_n$ be a basis for the right-invariant Lie algebra of G, and let $D=X_1^2+\cdots+X_n^2+X$, where X is in the Lie algebra. Let T be a bounded strongly continuous representation of G on a Banach space $\mathfrak{V}$. Then the closure A of $dT(D)$ is precisely the infinitesimal generator (in the sense of Hille [9] and Yosida [23]) of a bounded strongly continuous one-parameter semigroup of operators on $\mathfrak{V}$. The resolvent $R_\lambda=(\lambda-A)^{-1}$ for $\lambda>0$ is $T(k_\lambda)$, where k_λ is in $L_1(G)$.*

Proof. First, we shall show that $dT(D)-\lambda$ has a dense range. To do so, we show that any continuous linear functional ξ which annihilates the range must be 0. For if x is in $\mathfrak{V}$, the equation

$$0=\xi(T((D-\lambda)\phi)x)=\int(D-\lambda)\phi(\sigma)\xi(T(\sigma)x)\,d\sigma,$$

which must hold for all ϕ in $C_0^\infty(G)$, says that the function $f(\sigma)=\xi(T(\sigma)x)$ is a weak solution of the elliptic equation $(D^+-\lambda)f=0$. By [10], f is analytic, and $(D^+-\lambda)f=0$ in the ordinary pointwise sense. But we shall prove that 0 is the only bounded solution of this equation, and in this proof we need consider only real functions. Let U be the open unit ball in a C^∞ coordinate neighborhood of e. Then the following Dirichlet problem has a solution (see [3]): for each continuous function θ on the boundary Γ of U, there is a unique continuous function g on $\bar{U}$ such that g agrees with θ on Γ and satisfies $(D^+-\lambda)g=0$ in U. If $\theta\geqq 0$, then $0\leqq g(e)\leqq\max\theta$, for g can have neither a strictly positive maximum nor a strictly negative minimum inside U, since $D^+g(\sigma)\leqq 0$ at a maximum and $D^+g(\sigma)\geqq 0$ at a minimum. By the Riesz-Markoff theorem, there is a positive measure ν on Γ such that $g(e)=\int_\Gamma\theta\,d\nu$. Now $\nu(\Gamma)<1$, since $g(e)<1$ when $\theta=1$ on all of Γ, again because g cannot have a strictly positive maximum in U. But since the function f considered above satisfies $(D^+-\lambda)f=0$ on all of G, then $f(\tau)=\int_\Gamma f(\sigma\tau)\,d\nu(\sigma)$ for all τ in G. Since f is bounded, $\|f\|_\infty\leqq\nu(\Gamma)\|f\|_\infty$, and $f=0$. So $f(e)=\xi(x)=0$ for all x in $\mathfrak{V}$. Therefore $\xi=0$, and we have proved that $dT(D)-\lambda$ has a dense range.

Next, we shall conclude the proof of Theorem 3.1 in the special case that $\mathfrak{V}$ is $C(G)$, the space of all continuous functions h on G vanishing at ∞, with the supremum norm, and $(T(\sigma)h)(\tau)=h(\sigma^{-1}\tau)$. Again by the maxi-

mum principle, $\| (A-\lambda)\phi \|_\infty \geqq \lambda \| \phi \|_\infty$ for all ϕ in $C_0^\infty(G)$. Since $A-\lambda$ has a dense range, $R_\lambda = (\lambda - A)^{-1}$ is an everywhere-defined operator with $\| R_\lambda \| \leqq 1/\lambda$. By Yosida's theorem [23], this means that A is the infinitesimal generator of a strongly continuous semigroup of contraction operators on $C(G)$. The operator R_λ is a bounded operator on $C(G)$ which commutes with right translations. An application of the Riesz-Markoff theorem shows that R_λ is left convolution by a finite regular measure μ_λ. A simple computation shows that on $G - \{e\}$, μ_λ is a weak solution of the elliptic equation $(\lambda - D)f = 0$. By [10], there is an analytic function k_λ on $G - \{e\}$, such that on $G - \{e\}$, μ_λ is given by $d\mu(\sigma) = k_\lambda(\sigma)\,d\sigma$. Therefore, on the whole of G,

$$d\mu_\lambda(\sigma) = a_\lambda d\delta(\sigma) + k_\lambda(\sigma)\,d\sigma,$$

where a_λ is a number, and δ is the unit mass at e. It is well-known that $a_\lambda = 0$. One way to see this is to consider the operator R of left convolution by μ_λ acting on the Hilbert space $L_2(G)$. If s is an integer $> n/4$ $(n = \dim G)$, by [14], R^s has only continuous functions in its range; and then by Theorem 4 of [13], R^s is a Carleman operator. In other words, R^s is left convolution by a function in $L_2(G)$; but it is also left convolution by a measure of the form $d\nu(\sigma) = a_\lambda{}^s d\delta(\sigma) + h_\lambda(\sigma)\,d\sigma$ with h_λ in $L_1(G)$. So $a_\lambda = 0$. For use in the next paragraph we note that $\| k_\lambda \|_1 \leqq 1/\lambda$ since $\| R_\lambda \| \leqq 1/\lambda$.

We return to a general representation T. We shall define R_λ as $T(k_\lambda)$, where k_λ is the function we have just constructed, and we shall prove that $R_\lambda = (\lambda - A)^{-1}$. But for x in $\mathfrak{V}$ and ϕ in $C_0^\infty(G)$,

$$R_\lambda(\lambda - A)T(\phi)x = T(k_\lambda * (\lambda - D)\phi)x = T(\phi)x.$$

Hence $R_\lambda = (\lambda - A)^{-1}$, since $\lambda - A$ is closed and has a dense range. Setting $M = \sup_{\sigma\in G} \| T(\sigma) \|$, we have $\| R_\lambda{}^q \| \leqq \| k_\lambda \|_1{}^q M \leqq M\lambda^{-q}$ for all integers $q > 0$. This shows (see [15]) that A is the infinitesimal generator of a bounded strongly continuous semigroup of operators on $\mathfrak{V}$.

In the course of the proof of Theorem 3.1 we have established the following corollary which we state briefly for use in Section 4.

COROLLARY 3.2. *In the notation of Theorem* 3.1, *if s is an integer $> n/4$, then $R_\lambda{}^s = T(h)$, where h is in both $L_1(G)$ and $L_2(G)$.*

4. CCR groups. Kaplansky [11] calls a locally compact group G a *CRR group* if for each function f in $L_1(G)$ and each strongly continuous irreducible unitary representation U of G, the operator $U(f)$ is completely

continuous. The letters CCR, referring to the group algebra $L_1(G)$, stand for completely continuous representation. We have the following criterion for a Lie group to be CCR.

THEOREM 4.1. *Let U be a strongly continuous unitary representation of a Lie group G. Let L be any element of the right-invariant enveloping algebra of G. If $dU(L)$ has an inverse which is contained in a completely continuous operator, then $U(f)$ is completely continuous for all f in $L_1(G)$. Conversely, suppose that $U(f)$ is completely continuous for all f in $L_1(G)$. Then the closure of $dU(\Delta-1)$ has a completely continuous inverse, where $\Delta = X_1^2 + \cdots + X_n^2$ and $X_1, \cdots, X_n$ is a basis for the right-invariant Lie algebra of G.*

Proof. Let B be the completely continuous operator containing the inverse of $dU(L)$. If ϕ is in $C_0^\infty(G)$, then $U(\phi)$ is completely continuous because $U(\phi) = BU(L\phi)$. But $C_0^\infty(G)$ is dense in $L_1(G)$, and the completely continuous operators are closed in the uniform operator topology. The converse direction follows immediately from Theorem 3.1.

THEOREM 4.2. *Let G be a Lie group, and let K be a compact subgroup of G. Suppose that U is a strongly continuous unitary representation of G whose restriction to K contains each irreducible representation of K only finitely many times. Then $U(f)$ is completely continuous for all f in $L_1(G)$. Suppose, further, that the restriction of U to K is contained in the regular representation of K. Let f be a function on G with compact support. If f has $2s$ continuous derivatives, where s is an integer $> 1/4$ times the dimension of K, then $U(f)$ is of Hilbert-Schmidt type. If f has $4s$ continuous derivatives, then $U(f)$ has an absolutely convergent trace.*

Proof. Let $X_1, \cdots, X_r$ be a basis for the right-invariant Lie algebra of K, and let $\Delta = X_1^2 + \cdots + X_r^2$. By Theorem 3.1, there is a function k in $L_1(K)$ such that $V(k)$ contains the inverse of $dU(\Delta-1)$, where V is the restriction of U to K. But $V(k)$ must be completely continuous because $L(k)$ is, where L denotes the left regular representation of K, and because each irreducible representation of K is contained in the left regular representation. Consequently, $U(f)$ is completely continuous for all f in $L_1(G)$ by Lemma 4.1.

Now suppose further that V is contained in L. According to Corollary 3.2, if s is an integer $> r/4$, then there is a function h in $L_2(K)$ such that $L(h)$ is the closure of the inverse of $dL((\Delta-1)^s)$. Since K is compact, $L(h)$ is of Hilbert-Schmidt type; and, a fortiori, $V(h)$ is also. Let f be a

function on G with compact support. If f has $2s$ continuous derivatives, then $U(f) = V(h)U((\Delta - 1)^s f)$, and so $U(f)$ is of Hilbert-Schmidt type. If f has $4s$ continuous derivatives, then $U(f) = [V(h)]^2 U((\Delta - 1)^{2s} f)$, and so $U(f)$ has an absolutely convergent trace.

We remark that in some sense f needs its derivatives only in the direction of K, but we do not make the remark precise.

If G is a connected semi-simple matrix group, then, according to a result of Harish-Chandra [7], the hypotheses of Theorem 4.2 hold for all strongly continuous irreducible unitary representations of G, where K is a maximal compact subgroup. An idea of Godement yields a much shorter proof of this fact [6]; a further simplification of Godement's proof is given in [20]. The conclusion in this case overlaps other results of Harish-Chandra [8]. As another example, Godement [6] has shown that a Lie group of the form $K \cdot A$, where K is compact and A is Abelian, satisfies the hypotheses of Theorem 4.2 for all strongly continuous irreducible representations. The Euclidean group of real n-space, and the inhomogeneous unitary group of complex n-space are examples of such groups.

We may also use Theorem 4.1 to show that certain Lie groups are not CCR groups.

THEOREM 4.3. *Let H be a closed subgroup of the general linear group of a finite-dimensional real vector space $\mathfrak{V}$. Let G be the corresponding inhomogeneous group; i.e. the group of all affine transformations $x \to Ax + b$, where A is in H and b is in $\mathfrak{V}$. Let $\mathfrak{V}^*$ be the dual space of $\mathfrak{V}$, and let $\mathfrak{M}$ be a conical (i.e. invariant under $\xi \to \lambda\xi$ for $\lambda > 0$) submanifold of $\mathfrak{V}^*$ invariant under H^*, the contragredient group of H. Let μ be a regular measure on $\mathfrak{M}$ whose null sets are invariant under H^* and also under the maps $x \to \lambda x$ for $\lambda > 0$. For σ in G, say $\sigma x = Ax + b$, let $U(\sigma)$ be the unitary operator on $L_2(\mathfrak{M}, \mu)$ mapping*

$$h(\xi) \to h(A^*\xi)[\exp(i\xi(b))][d\mu(A^*\xi)/d\mu(\xi)]^{\frac{1}{2}},$$

where A^* is the adjoint transformation to A. Then representation U has the property that there exists a function f in $L_1(G)$ such that $U(f)$ is not completely continuous.

Proof. Let Δ_H be the sum of the squares of the elements of a basis for the Lie algebra of H. Choose a positive definite inner product in $\mathfrak{V}$, and let Δ be the element of the enveloping algebra of the translation part of G corresponding to the Laplacian operator on $\mathfrak{V}$. Let N be the closure of

$dU(\Delta_H - 1)$, and M, the closure of $dU(\Delta)$. Then M is multiplication by the function $-r^2$ on $\mathfrak{V}^*$, where $r(\xi) = |\xi|$. Any one-to-one measurable transformation S of $\mathfrak{M}$ onto itself which preserves null sets of μ gives rise to a unitary operator $\hat{S}$ on $L_2(\mathfrak{M}, \mu)$ as follows:

$$(\hat{S}h)(\xi) = h(S\xi)[d\mu(S\xi)/d\mu(\xi)]^{\frac{1}{2}}.$$

If S_1 and S_2 commute, so do $\hat{S}_1$ and $\hat{S}_2$. For $\lambda > 0$, let T_λ be the transforma- of $\mathfrak{M}$ given by $T_\lambda(\xi) = \lambda\xi$. By the remark we have just made, $\hat{T}_\lambda$ commutes with $U(H)$, and therefore with N. Let ϕ be in $C_0^\infty(\mathfrak{M})$ with $\|\phi\|_2 = 1$. Then $\|N\hat{T}_\lambda\phi\|_2 = \|\hat{T}_\lambda N\phi\|_2 = \|N\phi\|_2$, and $\|M\hat{T}_\lambda\phi\|_2 \leqq \rho(\lambda)\|\hat{T}_\lambda\phi\|_2 = \rho(\lambda)$, where $\rho(\lambda)$ is the maximum of $|\xi|^2$ when $\lambda\xi$ is in the support of ϕ. Consequently, $(N+M)\hat{T}_\lambda\phi$ is bounded for $\lambda \geqq 1$. But the $\hat{T}_\lambda\phi$ for $\lambda \geqq 1$ are not contained in any compact set; in fact, a suitable subfamily forms an infinite orthonormal set. In other words, the inverse of $N+M$ is not contained in any completely continuous operator. Theorem 3.1 asserts that this fact implies the conclusion of the present theorem.

If the group H^* is transitive on the cone $\mathfrak{M}$, then the representation U of G is irreducible (see [12]), and hence G is not CCR. As examples of linear groups H such that H^* is transitive on a cone, we mention the (real or complex) general linear group, the (real or complex) unimodular group acting on a space of dimension $\geqq 2$, a non-compact pseudo-orthogonal group, and the group of transformations $x \to ax$ for $a > 0$ acting on the line. This last case shows that the group of transformations $x \to ax + b$ for $a > 0$ acting on the line is *not* CCR despite the contrary assertion by Gelfand and Neumark in the introduction to [4]. The next to last case shows that the inhomogeneous Lorentz group is not CCR. Theorem 4.3 says that the irreducible representation of this group over the light-cone with spin 0 (see [2] and [22]) does not universally send integrable functions on the group into completely continuous operators. The method of proof of Theorem 4.3 shows that the same is also true for irreducible representations of higher spin over the light-cone.

5. Counterexamples. A unitary representation of a Lie group does not always send symmetric elements of the enveloping algebra into operators essentially self-adjoint on the Gårding subspace. The first such counterexample was given by von Neumann (unpublished). Let G be the group of the Heisenberg commutation relations; that is to say, G is the 3-dimensional group of all real matrices of the form:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

This group G has an irreducible unitary representation on $L_2(-\infty, +\infty)$ whose infinitesimal operators are d/dx, ix, and i. In other words, the enveloping algebra of G maps onto all ordinary differential operators with polynomial coefficients, and there are many of these which are symmetric but not essentially self-adjoint.

In [17], Segal proved that the elements of the Lie algebra itself multiplied by i are always represented by operators essentially self-adjoint on the Gårding subspace. He also asserted in [17] that symmetric second order elements of the enveloping algebra are always represented by operators essentially self-adjoint on the Gårding subspace if the group is unimodular. However, L. Gross found an error in the proof, and this observation formed the starting point for our researches. (The statement on line 5 of p. 236 of [17] is incorrect, since the quantity on the preceding line is only $O(n)$.) In fact, we shall present a counterexample in the next paragraph even for a semi-simple group. The remainder of [17] is unaffected, since one may use instead Segal's theorem that central elements of the enveloping algebra are always represented by essentially self-adjoint operators if they are symmetric [18] (see a forthcoming note by Segal [19]).

Let G be the group of all 2×2 real unimodular matrices. Bargmann [1] has found all the irreducible unitary representations of this group. The one he denotes by $C^0{}_{1/4}$ acts on $L_2(M)$, where M is the real numbers modulo 2π, and is given infinitesimally by

$$dU(\Lambda_0) = -d/dx$$

$$dU(\Lambda_1) = \cos x\, d/dx - \tfrac{1}{2}\sin x$$

$$dU(\Lambda_2) = \sin x\, d/dx + \tfrac{1}{2}\cos x,$$

where we denote the representation by U. Let $A = \Lambda_0\Lambda_2 + \Lambda_2\Lambda_0$. Calculation shows

$$dU(A) = -2d/dx \sin x\, d/dx + \tfrac{1}{2}\sin x.$$

Let E be the operator with the same formula as $dU(A)$ but with domain $C_0{}^\infty(M)$; E and $dU(A)$ have the same closure. The operator E is not essentially self-adjoint because of the vanishing of $\sin x$. One way to see this is to consider the functions

$$f(x)=\begin{cases}\log|\sin x| & \text{for } -\frac{\pi}{2}\leqq x\leqq\frac{\pi}{2}\\ 0 & \text{elsewhere on } M,\end{cases}$$

and

$$g(x)=\begin{cases}1 & \text{for } 0\leqq x\leqq\pi\\ 0 & \text{elsewhere on } M.\end{cases}$$

Then the distribution derivative (see [16]) of f is the map

$$\phi\to \mathrm{P.V.}\int_{-\pi/2}^{\pi/2}\phi(x)\cos x/\sin x\,dx,$$

where P. V. means the Cauchy principal value of the integral. Hence the operator with the same formula as E applied to f in the sense of distributions yeilds the function

$$h(x)=\begin{cases}2\sin x+\frac{1}{2}\sin x\,f(x) & \text{for} -\frac{\pi}{2}\leqq x\leqq\frac{\pi}{2}\\ 0 & \text{elsewhere on } M.\end{cases}$$

Since f and h are both in $L_2(M)$, this means that $h=E^*f$. Similarly, $k=E^*g$, where

$$k(x)=\begin{cases}\frac{1}{2}\sin x & \text{for } 0\leqq x\leqq\pi\\ 0 & \text{elsewhere on } M.\end{cases}$$

But $(E^*f,g)-(f,E^*g)=\int_0^{\pi/2}2\sin x\,dx\neq 0$. Consequently E, and hence $dU(A)$, are not essentially self-adjoint.

To see how ellipticity prevents this sort of thing from happening, let B be an elliptic element in the enveloping algebra of G. By definition, $B=p(\Lambda_0,\Lambda_1,\Lambda_2)+$ lower order terms, where p is a homogeneous polynomial that never vanishes when its argument is a non-zero triple of real numbers. Then

$$dU(B)=p(-d/dx,\cos x\,d/dx,\sin x\,d/dx)+\text{lower order terms}$$

is an ordinary differential operator on M with a nowhere vanishing leading coefficient. In this case the conclusion of Theorem 2.2, that the closure of $dU(B)$ is the Hilbert space adjoint of its formal Lagrange adjoint, is well-known.

For another example of a symmetric second-order element of an enveloping algebra being represented by an operator which is not essentialy self-adjoint, let G be the $ax+b$ group. Let U be one of its two infinite dimensional irreducible unitary representations (see [12]). One version of U acts on $L_2(-\infty,+\infty)$ and has infinitesimal operators

$$dU(X) = d/dx \text{ and } dU(Y) = ie^x.$$

Then $dU(XY + YX) = 2ie^x\, d/dx + ie^x$, and by [21] (X, sec. 2) this operator has deficiency indices $(0,1)$, since e^{-x} is not integrable near $-\infty$ but is integrable near $+\infty$. Consequently, $dU(XY + YX)$ has no self-adjoint extension. Although G is not unimodular, this example can be converted into one for a unimodular group. A theorem of Gleason [5] shows that there is a unimodular group G_1 with a normal subgroup R isomorphic to the additive group of all real numbers such that $G \cong G_1/R$. Then U composed with the natural map $G_1 \rightarrow G$ gives a representation of G_1 with the same infinitesimal operators.

INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[1] V. Bargmann, "Irreducible unitary representations of the Lorentz group," *Annals of Mathematics*, vol. 48 (1947), pp. 548-640.

[2] ——— and E. P. Wigner, "Group theoretical discussion of relativistic wave equations," *Proceedings of the National Academy of Sciences*, vol. 34 (1946), pp. 211-223.

[3] L. Gårding, "Dirichlet's problem for linear elliptic partial differential equations," *Mathematica Scandinavia*, vol. 1 (1953), pp. 55-71.

[4] I. M. Gelfand and M. A. Neumark, *Unitäre Darstellungen der klassischen Gruppen*, Akademie-Verlag, Berlin, 1957.

[5] A. M. Gleason, "A note on locally compact groups," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 744-745.

[6] R. Godement, "A theory of spherical functions I," *Transactions of the American Mathematical Society*, vol. 73 (1952), pp. 496-556.

[7] Harish-Chandra, "Representations of a semisimple Lie group on a Banach space I," *ibid.*, vol. 75 (1953), pp. 185-243.

[8] ———, "Representations of semisimple Lie groups III," *ibid.*, vol. 76 (1954), pp. 234-253.

[9] E. Hille, *Functional analysis and semi-groups*, American Mathematical Society Colloquium Publications 31, New York, 1948.

[10] F. John, "General properties of solutions of linear elliptic partial differential equations," *Proceedings of the Symposium on Spectral Theory and Differential Problems*, Stillwater, Oklahoma, 1951.

[11] I. Kaplansky, "The structure of certain operator algebras," *Transactions of the American Mathematical Society*, vol. 70 (1951), pp. 219-255.

[12] G. W. Mackey, "Induced representations of locally compact groups I," *Annals of Mathematics*, vol. 55 (1952), pp. 101-139.

[13] Edward Nelson, "Kernel functions and eigenfunction expansions," *Duke Mathematical Journal*, vol. 25 (1958), pp. 15-27.

[14] L. Nirenberg, "Remarks on strongly elliptic partial differential equations," *Communications on Pure and Applied Mathemtics*, vol. 8 (1955), pp. 649-675.

[15] R. S. Phillips, "Semi-groups of operators," *Bulletin of the American Mathematical Society*, vol. 61 (1953), pp. 16-33.

[16] L. Schwartz, *Théorie des distributions*, Hermann, Paris, 1950.

[17] I. E. Segal, "A class of operator algebras which are determined by groups," *Duke Mathematical Journal*, vol. 18 (1951), pp. 221-265.

[18] ———, "Hypermaximality of certain operators on Lie groups," *Proceedings of the American Mathematical Society*, vol. 3 (1952), pp. 13-15.

[19] ———, "A theorem on the measurability of group-invariant operators," to appear.

[20] W. F. Stinespring, "A semi-simple matrix group is of type I," *Proceedings of the American Mathematical Society*, vol. 9 (1958), pp. 965-967.

[21] M. H. Stone, *Linear transformations in Hilbert space and their applications to analysis*, American Mathematical Society Coloquium Publications 15, New York, 1932.

[22] E. Wigner, "On unitary representations of the inhomogeneous Lorentz group," *Annals of Mathematics*, vol. 40 (1939), pp. 149-204.

[23] K. Yosida, "On the differentiability and the representation of one-parameter semigroup of linear operators," *Journal of the Mathematical Society of Japan*. vol. 1 (1948), pp. 15-21.

KRONECKERIAN MODEL OF FIELDS OF ELLIPTIC MODULAR FUNCTIONS.*[1]

By JUN-ICHI IGUSA.

In our previous paper [7-III], we gave a geometric construction of the field of elliptic modular functions of an arbitrary level n for any characteristic which does not divide n and we discussed its basic properties. We shall now piece together the fields of modular functions of level n in different characteristics so that we get a fibre system parametrized by the ring of rational integers. More precisely, we shall construct a non-singular projective model of the field of modular functions of level n in characteristic zero over the field of rational numbers such that its reduction with respect to every prime number p not dividing n is a non-singular projective model of the field of modular functions of level n in characteristic p over the prime field. We can also say, more suggestively, that *the compactified fundamental domain of the congruence modular group of level n admits a "characteristic p deformation," provided p does not divide n.* At any rate, the construction is unique up to a biregular transformation. The birational geometry of this type of fibre systems explains, for instance, why the absolute invariants of three elliptic curves obtained from the invariant transformation equations of degree 11, 17, 19 are rational numbers with denominators exactly at these prime numbers. Moreover, the existence of the fibre system guarantees that the Petersson conjecture [10] on the eigen values of Hecke operators operating on cusp forms is true for dimension -2. As we know, the validity of this conjecture for *almost all* prime numbers was proved by Eichler [4] in a slightly less general case, which was later generalized by Shimura [12]. We like to mention, however, that the validity for *individual* prime numbers was an open question.

1. **Preparations.** Let Z be the ring of rational integers and let Q be its field of fractions. We shall denote the algebraic closure of Q by Q_0. Also,

* Received September 2, 1958.

[1] This work was partially supported by a research grant of the National Science Foundation. The result of this paper was communicated to Professor Weil in November, 1957.

we fix a positive integer n once for all and we shall denote the field of n-th roots of unity over Q by Q_n. Let j be transcendental over Q and pick an elliptic curve A_j which is defined over $Q(j)$ and which has j as its absolute invariant. We note that A_j is unique only up to an isomorphism. Let Ω be the group of points of A_j of order n. We shall denote by Ku the identification mapping of two points of opposite signs of an elliptic curve. Then $Q_0(j, Ku(\Omega))$ is what we called the field of modular functions of level n in characteristic zero.[2] In fact, if we extend Q_0 to the field of complex numbers, we get the classical field of modular functions of level n. We know that the field $Q(j, Ku(\Omega))$ does not depend on the choice of A_j and that Q_n is the algebraic closure of Q in $Q(j, Ku(\Omega))$.

Now, pick two generators ω_1 and ω_2 of Ω and let j_n be the absolute invariant of the factor group of A_j by the cyclic group generated by ω_1. We shall show that the field $K = Q(j, j_n, Ku(\omega_2))$ depends neither on the choice of A_j nor on the choice of the generators ω_1 and ω_2 of Ω. Suppose first that ω_1' and ω_2' are two generators of Ω. Then we can transform the pair (ω_1, ω_2) either to (ω_1', ω_2') or to $(-\omega_1', -\omega_2')$ by an automorphism of $Q(j, \Omega)$ over $Q(j)$ [7-III, Theorem 3]. If j_n' is the absolute invariant of the factor group of A_j by the cyclic group generated by ω_1', this automorphism transforms $(j_n, Ku(\omega_2))$ to $(j_n', Ku(\omega_2'))$. Therefore, if we fix A_j, the field K is unique up to an isomorphism over $Q(j)$. Next, let B_j be another elliptic curve which is defined over $Q(j)$ and which has j as its absolute invariant. Let ω_1' and ω_2' be the images of ω_1 and ω_2 under an isomorphism between A_j and B_j. Then ω_1' and ω_2' generate the group of points of B_j of order n. Let j_n' be the absolute invariant of the factor group of B_j by the cyclic group generated by ω_1'. Then the conjugate of ω_1 over $Q(j, j_n)$ is simply another generator of the cyclic group generated by ω_1 [7-III, remark after Theorem 7]. The same is true for ω_1' instead of ω_1 over $Q(j, j_n)$, hence j_n' is contained in $Q(j, j_n)$. Since $Ku(\omega_2')$ is also rational over $Q(j, Ku(\omega_2))$, we see that $Q(j, j_n', Ku(\omega_2'))$ is contained in $Q(j, j_n, Ku(\omega_2)) = K$. Since the situation is symmetric, we get $Q(j, j_n', Ku(\omega_2')) = K$. This proves the assertion.

We have thus shown that *the field K is an intrinsically defined algebraic extension of $Q(j)$*. If we apply the Galois theory [7-III, Theorem 3], we see that $Q(j, Ku(\Omega))$ and $Q(j)$ are respectively the compositum and the inter-

[2] The properties of fields of modular functions we need in this paper are discussed purely geometrically in [7-III]. If the reader does not mind using transcendental theory in the case of characteristic zero, he can refer to the classical treatment like [14]. However, at least at present, the theory of modular functions in positive characteristic is indispensable to prove our main theorem.

section of K and $Q_n(j)$. Therefore K and $Q_n(j)$ are linearly disjoint over $Q(j)$, hence K and Q_n are linearly disjoint over Q. In particular, K is a regular extension of Q.

Let p be a prime number and extend the p-adic valuation of Q to $Q(j)$ by the Gaussian definition. Let $Q(j)_p$ be the corresponding valuation ring of $Q(j)$. If F is the prime field of characteristic p, i.e., if we put $F=Z/pZ$, and if j' is transcendental over F, then $Q(j)_p$ is the specialization ring of the specialization $Z[j]\rightarrow F[j']$. This being remarked, we shall prove the following lemma:

LEMMA 1. *If p does not divide the level n, the integral closure R of $Q(j)_p$ in K is an unramified discrete valuation ring.*

Proof. Suppose first that p is different from 2. Let λ be a root of the equation

$$2^8(T^2-T+1)^3-jT^2(T-1)^2=0$$

and let R_λ be an extension of $Q(j)_p$ to the field $K(\lambda)$. It is then sufficient to show that this valuation ring is unique and unramified. It is equivalent to say that the residue field of R_λ is of degree $[K(\lambda):Q(j)]$ over $F(j')$. In fact, we have only to recall the well-known relation between total degree and local degrees composed of residue degrees and ramification indices [cf. 18]. Let λ' be the specialization of λ over the residue homomorphism of R_λ. Since 2 is a unit in $Q(j)_p$, hence also in R_λ, we see that λ' is transcendental over F and we have $[F(\lambda'):F(j')]=[Q(\lambda):Q(j)]$. Therefore, we have only to show that the residue field of R_λ is of degree $[K(\lambda):Q(\lambda)]$ over $F(\lambda')$. Consider a plane cubic A_λ which is defined over $Q(\lambda)$ by the equation $Y^2Z=X(X-Z)(X-\lambda Z)$. We introduce a group law in A_λ, say, with reference to the point $(0,1,0)$. We know that A_j and A_λ are isomorphic over some quadratic extension of $Q(\lambda)$. Let ϖ_1 and ϖ_2 be the images of ω_1 and ω_2 under an isomorphism between A_j and A_λ. Then ϖ_1 and ϖ_2 generate the group of points of A_λ of order n. Moreover, we have $Q(\lambda,Ku(\varpi_2))=Q(\lambda,Ku(\omega_2))$, hence $Q(\lambda,j_n,Ku(\varpi_2))=Q(\lambda,j_n,Ku(\omega_2))=K(\lambda)$. Here j_n can be considered as the absolute invariant of the factor group of A_λ by the cyclic group generated by ϖ_1. Let $(\lambda',j_n',Ku(\varpi_2)')$ be the specialization of $(\lambda,j_n,Ku(\varpi_2))$ over the residue homomorphism of R_λ. Then A_λ is reduced to a plane cubic $A_{\lambda'}$ which is defined over $F(\lambda')$ by the equation $Y^2Z=X(X-Z)(X-\lambda'Z)$. We introduce a group law in $A_{\lambda'}$ with reference to the point $(0,1,0)$. Let (ϖ_1',ϖ_2') be a specialization of (ϖ_1,ϖ_2) over the above specialization. Then ϖ_1' and ϖ_2' generate the group of points of $A_{\lambda'}$ of order n. Moreover, j_n' is the absolute invariant of the factor group of $A_{\lambda'}$ by the cyclic group

generated by ϖ_1', while we have $Ku(\varpi_2)' = Ku(\varpi_2')$. On the other hand, from the Galois theory [7-III, Theorem 1] we conclude that

$$[F(\lambda', j_n', Ku(\varpi_2')) : F(\lambda')] \text{ and } [Q(\lambda, j_n, Ku(\varpi_2)) : Q(\lambda)]$$

are equal. Therefore $F(\lambda', j_n', Ku(\varpi_2'))$ must coincide with the residue field of R_λ and it is of degree $[K(\lambda) : Q(\lambda)]$ over $F(\lambda')$. This completes the proof in the case p is different from 2. Suppose next that p is 2. Let μ be a root of the equation

$$3^3 T^3 (T^3 + 2^3)^3 - j(T^3 - 1)^3 = 0$$

and let R_μ be an extension of $Q(j)_p$ to $K(\mu)$. Let μ' be the specialization of μ over the residue homomorphism of R_μ. Then, by a similar reason as in the previous case, it is sufficient to show that the residue field of R_μ is of degree $[K(\mu) : Q(\mu)]$ over $F(\mu')$. In order to prove this fact, we consider a plane cubic A_μ which is defined over $Q(\mu)$ by the equation $X^3 + Y^3 + Z^3 = 3\mu XYZ$. We introduce a group law in A_μ, say, with reference to the point $(-1, 1, 0)$. We know that A_j and A_μ are isomorphic over some quadratic extension of $Q(\mu)$. Let ϖ_1 and ϖ_2 be the images of ω_1 and ω_2 under an isomorphism between A_j and A_μ. Then we have $Q(\mu, j_n, Ku(\varpi_2)) = K(\mu)$. Let $(\mu', j_n', Ku(\varpi_2)')$ be the specialization of $(\mu, j_n, Ku(\varpi_2))$ over the residue homomorphism of R_μ. Let (ϖ_1', ϖ_2') be a specialization of (ϖ_1, ϖ_2) over this specialization. Then, from the Galois theory [7-III, Theorem 2] we conclude that $F(\mu', j_n', Ku(\varpi_2'))$ is the residue field of R_μ and it is of degree $[K(\mu) : Q(\mu)]$ over $F(\mu')$.

Now, consider the ring $Z[j]$ of polynomials in j with integral rational coefficients and take its integral closure S in K. Then S is a $Z[j]$-module and a general theorem guarantees the finiteness of S over $Z[j]$. In this case, however, the proof is quite simple. Pick a base $\theta_1, \theta_2, \cdots$ of K over $Q(j)$ from S and let d be the discriminant of the base. Then d is different from zero and S is contained in the finite $Z[j]$-module generated by $\theta_1/d, \theta_2/d, \cdots$. Since $Z[j]$ is Noetherian, we see that S itself is a finite $Z[j]$-module. If we treat j and $1/j$ symmetrically, we are forced to introduce the integral closure N of $Z[1/j]$ in K. Then N is a finite $Z[1/j]$-module. On the other hand, since $Z[j]$ and $Z[1/j]$ are contained in $Q(j)_p$, both S and N are contained in the integral closure R of $Q(j)_p$ in K. If p does not divide n, we know by Lemma 1 that R is an unramified discrete valuation ring, i.e. that the ideal of non-units of R is pR. We shall show that we have $pR \cap S = pS$. Let f be an element of $pR \cap S$. Then f/p is contained in R. Since R is the only discrete valuation ring of K which comes from a minimal prime ideal of pS, we see that f/p is contained in every discrete valuation ring of K which comes

from a minimal prime ideal of S. However, since S is an integrally closed Noetherian domain, the intersection of these valuation rings coincides with S by a theorem of Krull [cf. 18]. Therefore f/p is an element of S, hence f is an element of pS. The converse is obvious. Similarly, we get $pR\cap N=pN$. In particular, pS and pN are prime ideals of S and N. Let K' be the residue field of R, i. e., put $K'=R/pR$. If S' and N' are the images of S and N under the residue homomorphism $R\rightarrow K'$, i. e., if we put $S'=S/pS$ and $N'=N/pN$, then K' is the common field of fractions of S' and N'. Now, we shall prove the following lemma:

LEMMA 2. *The field $K'=R/pR$ is a regular extension of F. Moreover, the compositum of K' and the algebraic closure k of F is the field of modular functions of level n in characteristic p.*

Proof. We shall use the same notation as in the proof of Lemma 1. First we shall show that K' is regular over F. It is sufficient to show that the residue fields R_λ/pR_λ and R_μ/pR_μ are both regular over F. Let F_n be the field of n-th roots of unity over F. If we apply the Galois theory [7-III, Theorem 1], we see that $R_\lambda/pR_\lambda=F(\lambda',j_n',Ku(\varpi_2'))$ and $F_n(\lambda')$ are linearly disjoint over $F(\lambda')$. We know that their compositum is regular over F_n, hence R_λ/pR_λ is regular over F. In the same way, we see that R_μ/pR_μ is regular over F. Next we shall show that the compositum kK' is the field of modular functions of level n in characteristic p. Pick an elliptic curve $A_{j'}$ which is defined over $F(j')$ and which has j' as its absolute invariant. Let Ω' be the group of points of $A_{j'}$ of order n. Suppose that p is different from 2. We know that $A_{j'}$ and $A_{\lambda'}$ are isomorphic over some quadratic extension of $F(\lambda')$. Let ω_1' and ω_2' be the images of ϖ_1' and ϖ_2' under an isomorphism between $A_{j'}$ and $A_{\lambda'}$. Then ω_1' and ω_2' generate the group Ω' and j_n' can be considered as the absolute invariant of the factor group of $A_{j'}$ by the cyclic group generated by ω_1'. Moreover, by the Galois theory [7-III, Theorem 3] we have $k(j',j_n',Ku(\omega_2'))=k(j',Ku(\Omega'))$, and this is the field of modular functions of level n in characteristic p [cf. 7-III]. Therefore, if we put $K''=F(j',j_n',Ku(\omega_2'))$, we have only to show $kK'=kK''$. Since we have $F(\lambda',Ku(\omega_2'))=F(\lambda',Ku(\varpi_2'))$, we get $F(\lambda',j_n',Ku(\omega_2'))=F(\lambda',j_n',Ku(\varpi_2'))$, hence $K''(\lambda')=R_\lambda/pR_\lambda=K'(\lambda')$. Now, in case n is even, we have $K'(\lambda')=K'$ and $K''(\lambda')=K''$, hence $K'=K''$. In case n is odd, the situation is rather delicate. Consider the compositums F_nK'' and $F_nK''(\lambda')$ and put $\Sigma=F_nK''$. Then Σ and $F_n(\lambda')$ are linearly disjoint over $F_n(j')$ with $F_nK''(\lambda')$ as their compositum and the ramification index of Σ over $F_n(j')$ at $j'=\infty$ is n [7-III, Theorem 6]. We shall show that Σ is characterized by these properties.

Since $F_n(\lambda')$ is ramified over $F_n(j')$ at $j'=\infty$ with index 2 and since n is odd, we see that the inertia groups of $F_nK''(\lambda')$ over $F_n(j')$ at $j'=\infty$ are cyclic of order $2n$. The elements of order 2 in these groups generate a unique normal subgroup of the Galois group of $F_nK''(\lambda')$ over $F_n(j')$ and Σ is precisely the corresponding invariant subfield of $F_nK''(\lambda')$. Hence Σ is unique. We shall show that F_nK' has the same properties as Σ. We have seen in the proof of Lemma 1 that F_nK' has the first property. On the other hand, F_nK' and Σ both contain the Galois extension of $F_n(j')$ generated by j'_n. This implies that the ramifications of F_nK' and Σ over $F_n(j')$ are the same except possibly at $j'=\infty$ [cf. 7-III, remark after Theorem 7]. If the ramifications are different, the ramification index of F_nK' over $F_n(j')$ at $j'=\infty$ will be $2n$. Then the genus of K' will be larger than the genus of Σ, which is equal to that of K [7-III, Theorem 5]. This is a contradiction [cf. 1]. Hence we get $F_nK'=\Sigma$. Suppose finally that p is 2. Define the generators ω_1' and ω_2' of Ω' and the field K'' as in the previous case. Then the compositum kK'' is the field of modular functions of level n in characteristic 2, and we get $K''(\mu')=R_\mu/pR_\mu=K'(\mu')$. Now, in case n is a multiple of 3, we have $F_3K'(\mu')=F_3K'$ and $F_3K''(\mu')=F_3K''$, hence $F_3K'=F_3K''$. If n is not a multiple of 3, then $F_{3n}K''$ and $F_{3n}(\mu')$ are linearly disjoint over $F_{3n}(j')$ with $F_{3n}K''(\mu')$ as their compositum and the ramification index of $F_{3n}K''$ over $F_{3n}(j')$ at $j'=\infty$ is n. As before, these properties characterize $F_{3n}K''$ and the first property is satisfied by $F_{3n}K'$. On the other hand, $F_{3n}K'$ and $F_{3n}K''$ both contain the Galois extension of $F_{3n}(j')$ generated by j_n' from which we conclude that the second property is also satisfied by $F_{3n}K'$. Hence we get $F_{3n}K'=F_{3n}K''$.

We note that the main complications of the proofs of the two lemmas result from the inclusion of the two cases $p=2,3$. If the reader does not mind excluding these cases, we can give very simple proofs.

2. Kroneckerian model. Let K be, as in the previous section, the intrinsically defined algebraic extension of $Q(j)$ depending on n. Also, let S and N be the integral closures of $Z[j]$ and $Z[1/j]$ in K. The *Kroneckerian model of fields of modular functions of level n* is, then, the union $\mathfrak{M}$ of specialization rings of S and N. We note that the union $\mathfrak{D}$ of specialization rings of $Z[j]$ and $Z[1/j]$ is the so-called universal projective straight line and the Kroneckerian model $\mathfrak{M}$ is the "derived normal model" of $\mathfrak{D}$ in K. At any rate, if we classify specialization rings of $\mathfrak{M}$ according to the characteristics of image fields, the model $\mathfrak{M}$ splits into enumerably many "local models" as follows:

$$\mathfrak{M} = \mathfrak{M}_0 + \sum_p \mathfrak{M}_p.$$

Now, following Zariski [17, see also 9], we shall construct a projective model of $\mathfrak{M}_0$ such that $\mathfrak{M}_p$ will become the union of specialization rings of points of its reduction with respect to p [cf. 11], and we shall investigate the local models closely.

Let m be a positive integer and let S_m be the set of elements f of S such that f/j^m is integral over $Q[1/j]$. Then, the sequence $S_1, S_2, \cdots$ determines an increasing filtration of the Z-module S. Also, it is clear that we have $pS \cap S_m = pS_m$. Let f be an element of S and let $f^t + c_1(j)f^{t-1} + \cdots + c_t(j) = 0$ be an irreducible monic equation for f over $Z[j]$. Then f/j^m is integral over $Q[1/j]$ if and only if we have deg. $c_i(j) \leqq mi$ for $i = 1, 2, \cdots, t$. This implies that f/j^m is integral over $Z[1/j]$, hence we have $S_m = S \cap j^m N$. Put $N_m = N \cap (1/j)^m S$. Then, the sequence $N_1, N_2, \cdots$ determines an increasing filtration of the Z-module N and we have $pN \cap N_m = pN_m$. Moreover, the multiplication by j^m is an isomorphism of N_m to S_m. Now, assume that p does not divide the level n and let S'' and N'' be the integral closures of $F[j']$ and $F[1/j']$ in K'. Here F, j' and K' are defined in the previous section. We can consider S'' and N'' as the integral closures of $S' = S/pS$ and $N' = N/pN$ in K'. Similarly as above, put $S''_m = S'' \cap (j')^m N''$ and $N''_m = N'' \cap (1/j')^m S''$. Then, we get increasing filtrations of the F-modules S'' and N'' and the multiplication by $(j')^m$ is an isomorphism of N''_m to S''_m. On the other hand, let S'_m and N'_m be the images of S_m and N_m under the residue homomorphism $R \to R/pR = K'$. Here R is defined in Lemma 1. Then, we get increasing filtrations of the F-modules S' and N'. Also, it is clear that S'_m is contained in S''_m and N'_m is contained in N''_m. Since we have $S'_m = S_m/pS_m$, the rank of S'_m as an F-module is equal to the rank of S_m as free Z-module. Similarly, the rank of N'_m is equal to the rank of N_m. Since S_m and N_m are isomorphic, these ranks are the same. Now, from Lemma 2 and from our previous result [7-III, Theorem 5] we conclude that K and K' have the same genus. Therefore, from the Riemann-Roch theorem [cf. 15] we conclude that S_m and S''_m have the same rank at least when $m[K: Q(j)]$ is greater than the degree of the canonical divisor of K. Actually, this condition is always satisfied [7-III, Theorem 4, Theorem 5]. Therefore, we get $S'_m = S''_m$ and $N'_m = N''_m$ for all m, hence $S' = S''$ and $N' = N''$. In other words, *the integral domains S' and N' are integrally closed in K'.* This is a key point.

Now, it is clear that S_m contains $1, j, \cdots, j^m$ and N_m contains $1, 1/j, \cdots, (1/j)^m$. Also, we know that S is a finite $Z[j]$-module and N is a finite

$Z[1/j]$-module. Therefore, if we take m sufficiently large, we have $Z[S_m]=S$ and $Z[N_m]=N$, hence applying the residue homomorphism $R\to K'$, we get $F[S'_m]=S'$ and $F[N'_m]=N'$. This being remarked, let $f_0, f_1,\cdots,f_r$ be a base of the free Z-module S_m. Let C be a curve in the projective space over Q of dimension r with $M=(f_0,f_1,\cdots,f_r)$ as a generic point over Q. It is clear that, once m is fixed, this curve C is uniquely determined up to a projective transformation with integral unimodular coefficient-matrix. We shall show that we can normalize C to the extent that we have $f_0=1, f_1=j,\cdots, f_m=j^m$. We have only to show that the free Z-module generated by $1,j,\cdots,j^m$ is a direct summand of S_m. If it is not so, we can find a prime number p, which might divide n, such that the images of $1,j,\cdots,j^m$ under the residue homomorphism $S_m\to S_m/pS_m$ are no more independent over F. On the other hand, since $Z[j]$ is integrally closed in $Q(j)$, we obviously have $pS\cap Z[j]=pZ[j]$. Therefore, the image of j is transcendental over F, and thus we get a contradiction.

We shall now translate some ring-theoretic properties of S and N into geometric properties of C. We shall first show that C is non-singular. If we take the first co-ordinate hyperplane as a plane at infinity, the corresponding affine co-ordinate ring is simply the tensor product $Q\otimes S$, which is the integral closure of $Q[j]$ in K. Therefore, this affine representative is normal over Q, hence non-singular. If we take the $(m+1)$-th co-ordinate hyperplane as a plane at infinity, the corresponding affine co-ordinate ring is simply the tensor product $Q\otimes N$, and this is the integral closure of $Q[1/j]$ in K. Therefore, this affine representative is also normal over Q, hence non-singular. We note that these open sets already cover the entire curve C. Hence C is non-singular. In the following we shall fix this open covering of C.

We shall next show that, as long as p does not divide n, the reduction C_p of C with respect to p remains non-singular. We know that in such a case pS is a prime ideal of S and that the field of fractions K' of $S'=S/pS$ is regular over F. Therefore, the reduction of one open set of C with respect to p is an irreducible affine curve defined over F. Moreover, since we have $F[S'_m]=S'$ and since S' is integrally closed in K', this curve is normal over F, hence non-singular. In a similar way, we see that the reduction of other open set of C with respect to p is non-singular. These two affine curves determine an open covering of C_p, hence C_p is non-singular. We have thus proved the following theorem the first part of which is clear from the construction:

THEOREM 1. *There exists a non-singular projective model C of the*

field K over Q such that the local model $\mathfrak{M}_p$ is the union of specialization rings of points of its reduction C_p with respect to p. If p does not divide the level n, then C_p is a non-singular projective model of the field K' over F.

We note that in proving this theorem we made a full use of the theory of modular functions in arbitrary characteristic. Conversely, many of the theorems in characteristic p are contained in this theorem. We regard this theorem as one of the fundamental theorems in the theory of elliptic modular functions.

3. A digression. In the previous section, we defined the Kroneckerian model $\mathfrak{M}$ of fields of modular functions of level n. The union $\mathfrak{M}_n$ of local models $\mathfrak{M}_p$ for p dividing n may be called the *frontier* of $\mathfrak{M}$, because *the reduction of C with respect to such p is reducible.* In fact, the field K contains the field $Q(j, j_n)$. Here j_n is the absolute invariant of the factor group of A_j by its cyclic subgroup of order n. If, therefore, we can show that the extension of $pZ[j]$ to the integral closure of $Z[j]$ in $Q(j, j_n)$ is not unique, then pS will be divisible by more than one minimal prime ideal of S and, consequently, the reduction of C with respect to p will contain the same number of components. In order to show that the extension is not unique, we recall that j_n and j are related by an equation $\Phi_n(X, Y) = 0$ over Z known as the *invariant transformation equation* of *degree n*. Moreover [cf. 3], if p^e is the p-primary part of n and if we put $n = n'p^e$, then $\Phi_n(X, Y)$ splits modulo p as follows:

$$\Phi_n(X, Y) \equiv \Phi(X^{p^e}, Y)\Phi(X, Y^{p^e}) \cdot \prod_{i=1}^{e-1} \Phi(X^{p^{e-i-1}}, Y^{p^{i-1}})^{p-1} \mod p.$$

Here $\Phi(X, Y) = 0$ is the invariant transformation equation of degree n', which remains absolutely irreducible modulo p [7-III, remark after Theorem 7]. Therefore, the complete set of conjugates of j_n over $Q(j)$ splits modulo p into $e+1$ complete sets of conjugates over $F(j')$ among which $e-1$ sets appear $(p-1)$-times. This is more than what we actually need here.

Now, since the equation $\Phi_n(X, Y) = 0$ is absolutely irreducible in characteristic zero, it defines a curve Φ_n over Q in the product $D \times D$ of two projective straight lines. In the above discussion, we used a *biregular property* of Φ_n or, more precisely, its locus variety in the product $\mathfrak{D} \times \mathfrak{D}$. We shall now discuss a *birational property* of Φ_n in case n is a prime number.

THEOREM 2. *Let Γ be an arbitrary projective curve which is birationally equivalent to the curve Φ_p over some extension of Q. Then, unless Γ is of*

genus zero, its reduction modulo p is either reducible or an irreducible curve of a smaller genus.

Proof. If we put $n'=e=1$ in the congruence relation we mentioned before, we get $\Phi_p(X,Y)\equiv(X^p-Y)(X-Y^p)\bmod p$. We observe that the two curves in characteristic p defined inhomogeneously by $X^p-Y=0$ and $X-Y^p=0$ on the product $D_p\times D_p$ of two projective straight lines are non-singular and of genus zero. Moreover, they intersect transversally at p^2+1 points, hence the reduction of Φ_p with respect to p is a "reducible curve" with ordinary double points. This being remarked, let Γ' be a reduction of Γ modulo p and assume that Γ' is an irreducible curve of the same genus as Γ. If we project Γ and Γ' generically to a plane, we get the same situation by plane curves. In the same way, if we transform the curve Φ_p by the complete linear system of cubic surfaces, or surfaces of a higher order, of the ambient projective space and then project the image curve generically to a plane, we get the following situation: There are two irreducible plane curves Γ and Φ which are birationally equivalent over a field with a discrete valuation. The reduction Γ' of Γ with respect to this valuation is an irreducible curve. The reduction Φ' of Φ with respect to the same valuation does not contain a straight line as a component and has ordinary double points. We can show, under this circumstance, that Γ' is birationally equivalent to a component of Φ' or it is of genus zero. Since the proof is almost the same as van der Waerden's proof of his Theorem 5 in [13], we shall not repeat it here. At any rate, in the present case, we know that Φ' consists of two curves of genus zero. Therefore Γ', hence also Γ, must be of genus zero. q. e. d.

According to the genus formula for the curve Φ_p [7-III, Theorem 7], there are five exceptional prime numbers, which are 2, 3, 5, 7, 13. Theorem 2 has a number-theoretic consequence, which we shall discuss after this general lemma:

LEMMA 3. *Let γ be a projective curve defined over Q. Then we can construct a non-singular projective model Γ of γ over Q such that its reduction with respect to a prime number p remains non-singular whenever the reduction γ' of γ is genus-preserving,* i.e. *irreducible and has the same genus as γ.*

Proof. Since the proof is similar to the proof of Theorem 1, we shall give only an outline. We note that our lemma could be stated more generally. Let $x=(x_0,x_1,\cdots)$ be a homogeneous generic point of γ over Q, and let S be the integral closure of $Z[x]$ in $Q(x)$. Then S is a finite $Z[x]$-module. Moreover, if S_m is the Z-module of homogeneous elements of S of degree m,

there exists a positive integer m_0 such that $Z[x_i^{-m}S_m]$ is the integral closure of $Z[x_i^{-1}x]$ in its field of fractions for $m \geqq m_0$ and for $x_i \neq 0$ [cf. 9]. On the other hand, since we have $pS \cap S_m = pS_m$, the image S'_m of S_m in S' has the same rang as $Q \otimes S_m$. Let S'' be the integral closure of S' in its field of fractions and let S''_m be its homogeneous part of degree m. Then S'_m is contained in S''_m. If γ' has the same genus as γ, by re-embedding γ, we can assume that $Q \otimes S_m$ and S''_m have the same rank for all m. Then, we get $S' = S''$. Now, as we remarked already, there exists a finite number of elements $\theta_1, \theta_2, \cdots$ of S such that we have $S = Z[x]\theta_1 + Z[x]\theta_2 + \cdots$. Let m_1 be the maximum of maximal degrees of $\theta_1, \theta_2, \cdots$. Then, we can show that $F[S'_m]$ is integrally closed in its field of fractions for $m \geqq m_1$. Thus S_m for $m \geqq \max(m_0, m_1)$ defines a non-singular projective model Γ of γ over Q, and this Γ has the required property. q. e. d.

If we apply this lemma to the curve Φ_n, we see [7-III, Theorem 7] that we can find its non-singular projective model Γ over Q which remains non-singular for every reduction with respect to a prime number not dividing n. Therefore, if Φ_n is of genus one, the absolute invariant of Γ, which we can call the absolute invariant of Φ_n, must be a rational number whose denominator is composed of prime factors of n. If n itself is a prime number p, Theorem 2 shows that p must appear in the denominator. In this way, we get the following.

COROLLARY. *If the curve Φ_p is of genus one, its absolute invariant is a rational number and its denominator is of the form p^e with $e \geqq 1$.*

We know that the curve Φ_p is of genus one only in the three cases $p = 11$, 17, 19. Actually, after some rather complicated calculation, we can show that the corresponding three absolute invariants are

$$-2^{12}31^3 11^{-5} \qquad -3^3 11^3 17^{-4} \qquad -2^{18}7^3 19^{-3}.$$

The reader might think that Theorem 2 and hence the above corollary could be generalized to the case of a non-prime level. However, the situation is more delicate. In fact, the absolute invariants of Φ_n for $n = 14$, 15, 20, 21, 24, 27, 32, 36, 49 [7-III, Theorem 7] are the following:

$$\begin{array}{ccccc} 5^3 43^3 2^{-6}7^{-3} & 13^3 37^3 3^{-4}5^{-4} & 2^4 11^3 5^{-2} & 193^3 3^{-4}7^{-2} & \\ 2^4 13^3 3^{-2} & 0 \quad 2^6 3^3 & 0 & & -3^3 5^3. \end{array}$$

This table shows that not all prime factors of n appear in the denominator. We also note that $2^6 3^3$ and 0 are known as harmonic and equianharmonic cases [cf. 7-III] while, as we can see easily, the last case $-3^3 5^3$ is the case where

the curve has $\frac{1}{2}\cdot(1+(-7)^{\frac{1}{2}})$ as a "complex multiplication." On the other hand, the field of modular functions of level 6 is of genus one and its absolute invariant is zero. In fact, the field admits $LF(2,6)$ as a group of automorphisms, which is an extension of an Abelian group of type $(6,2)$ by a cyclic group of order 6. Since this is the only one metacyclic decomposition of $LF(2,6)$, the curve has sixth roots of unity as complex multiplications [cf. 16]. This shows that we have an equianharmonic case, hence the absolute invariant is zero.

4. Modular correspondences. We shall now discuss modular correspondences and, in particular, the eigen value of modular correspondences of prime degrees operating on differentials of the first kind. As before, let j be transcendental over Q and let A_j be an elliptic curve which is defined over $Q(j)$ and which has j as its absolute invariant. Also, let ω_1 and ω_2 be the generators of the group Ω of points of A_j of order n. We pick a generic point M over Q of the curve C constructed in Section 2 such that we have $Q(M)=Q(j,j_n,Ku(\omega_2))$. Here j_n is the absolute invariant of the factor group of A_j by the cyclic subgroup generated by ω_1. These being recalled, pick a positive integer m which is arbitrary provided it is relatively prime to n. Let j^* be a root of the invariant transformation equation $\Phi_m(X,j)=0$ of degree m and let A_{j^*} be the generic specialization of A_j over the specialization $j\to j^*$ with reference to Q. Then, there exists a homomorphism of A_j to A_{j^*} whose kernel is a cyclic group of order m. Let $\omega_1{}^*$ and $\omega_2{}^*$ be the images of ω_1 and ω_2 under this homomorphism. Since m is relatively prime to n, these images generate the group, say Ω^*, of points of A_{j^*} of order n. Let $j_n{}^*$ be the absolute invariant of the factor group of A_{j^*} by the cyclic subgroup generated by $\omega_1{}^*$. We shall show that $(j^*,j_n{}^*,Ku(\omega_2{}^*))$ is a generic specialization of $(j,j_n,Ku(\omega_2))$ over Q. Let $(\omega_1{}'',\omega_2{}'')$ be a specialization of (ω_1,ω_2) over the specialization $j\to j^*$ with reference to Q. Then, the specialization is generic and $\omega_1{}''$ and $\omega_2{}''$ generate the group Ω^*. Hence, by the Galois theory [7-III, Theorem 3] there exists an automorphism of $Q(j^*,\Omega^*)$ over $Q(j^*)$ which transforms $(\omega_1{}'',\omega_2{}'')$ either to $(\omega_1{}^*,\omega_2{}^*)$ or to $(-\omega_1{}^*,-\omega_2{}^*)$. Therefore $(j^*,j_n{}^*,Ku(\omega_2{}^*))$ is a generic specialization of $(j,j_n,Ku(\omega_2))$ over Q. Now, let M^* be a specialization of the point M over this specialization. Then M^* is unique and we have $Q(M^*)=Q(j^*,j_n{}^*,Kp(\omega_2))$. Moreover, from the same Galois theory we conclude that $Q(M,M^*)$ and $Q(j)$ are respectively the compositum and the intersection of $Q(M)$ and $Q(j,j^*)$. The situation remains true even after we extend Q to its algebraic closure Q_0. Therefore $Q(M,M^*)$ is a regular extension of Q and we have

$$[Q(M, M^*) : Q(M)] = [Q(j, j^*) : Q(j)] = m \cdot \prod_{p|m} (1 + p^{-1}).$$

Hence the point $M \times M^*$ of the product $C \times C$ has a locus X over Q. We note that the change of generators ω_1 and ω_2 of Ω amounts to replace the point $M \times M^*$ by its conjugate over $Q(j, j^*)$. Therefore the correspondence X is intrinsically defined. We call X the *modular correspondence* of *degree* m and of *level* n. If we replace M^* by its conjugate M^{**} over $Q(j^*)$, then the point $M \times M^{**}$ so obtained has a locus over the field Q_n of n-th roots of unity over Q. The modular correspondence X is, so-to-speak, singled out from these correspondences, which are sometimes called also modular correspondences.

Now, we shall assume that m is a prime number p. Remember that p does not divide n. Let C_p and X_p be the reductions of C and X with respect to p. Then C_p is a non-singular curve defined over the prime field F by Theorem 1. Let M_p be a generic point of C_p over F. If we denote by $(M_p)^p$ the point of C_p which is obtained by raising the co-ordinates of M_p to their p-th powers, the point $M_p \times (M_p)^p$ of the product $C_p \times C_p$ has a locus I over F. We call I the *Frobenius correspondence* of C_p [cf. 15]. On the other hand, let k be the algebraic closure of F. Then, with the notation of the proof of Lemma 2, we have $k(M_p) = k(j', j_n', Ku(\omega_2'))= k(j', Ku(\Omega'))$. If we write j_n' in the form $j_n(\omega_1')$, there exists an automorphism of $k(M_p)$ over $k(j')$ which transforms $(Ku(\omega_1'), Ku(\omega_2'))$ into $(Ku(\omega_2'), Ku(\omega_1'))$ [7-III, Theorem 3], hence $(j', j_n(\omega_1'), Ku(\omega_2'))$ into $(j', j_n(\omega_2'), Ku(\omega_1'))$. This automorphism transforms M_p to another generic point, say M_p^τ, of C_p over F. Let T be the locus of the point $M_p \times M_p^\tau$ over k. We note that T is not in general defined over F. At any rate, with these notations, we shall prove the following relation:

LEMMA 4. *If we denote by a right upper prime the effect of the permutation of factors of the product $C_p \times C_p$, we have*

$$X_p = I + T' \circ I' \circ T.$$

In other words, the modular correspondence of degree p splits modulo p into two Frobenius correspondences.

Proof. This important lemma was proved by Eichler [4] in a less general case and later by Shimura [12] in the above form for almost all p. Since our proof is quite similar to Shimura's proof, we shall give only an outline. If p is different from 2, we cover A_j by A_λ such that $A_{\lambda'}$ covers $A_{j'}$. The point is, of course, that $A_{\lambda'}$ is the reduction of A_λ while $A_{j'}$ is not in general the reduction of A_j with respect to p. In case p is 2, we cover A_j and

$A_{j'}$ by A_μ and $A_{\mu'}$ so that $A_{\mu'}$ is the reduction of A_μ with respect to 2. With the aid of these nice coverings, we can show that X_p consists of two parts one of which is I. Let $A_{j''}$ be the generic specialization of $A_{j'}$ over F which is obtained by replacing j' by $(j')^{1/p}$. Let α be a separable homomorphism of $A_{j'}$ to $A_{j''}$ of degree p [cf. 5; see also 8, section 5]. Then the other part of X_p is determined over k by $(j', j_n(\omega_1'), Ku(\omega_2')) \to ((j')^{1/p}, j_n(\alpha\omega_1'), Ku(\alpha\omega_2'))$. On the other hand, there exists an automorphism of $F(j', Ku(\Omega'))$ over $F(j')$ which transforms $(Ku(\omega_1'), Ku(\omega_2'))$ into $(Ku(\omega_1'), Ku(p\omega_2'))$ and its effect on the algebraic closure F_n of F in $F(j', Ku(\Omega'))$ is exactly the p-th power automorphism [7-III, Theorem 3]. Since $F(j', Ku(\Omega'))$ and k are linearly disjoint over F_n, the above automorphism of $F(j', Ku(\Omega'))$ and p-th power automorphism of k give rise to a semi-linear automorphism of $k(j', Ku(\Omega'))$ over k. Therefore, if T^p is the conjugate of T under the p-th power automorphism of k, then T^p is determined by

$$(j', j_n(\omega_1'), Ku(p\omega_2')) \to (j', j_n(\omega_2'), Ku(\omega_1')),$$

hence T is determined by

$$((j')^{1/p}, j_n(\omega_1')^{1/p}, Ku(p\omega_2')^{1/p}) \to ((j')^{1/p}, j_n(\omega_2')^{1/p}, Ku(\omega_1')^{1/p}).$$

However, since we have $j_n(\omega_1')^{1/p} = j_n(p\omega_1')^{1/p} = j_n(\alpha\omega_1')$ and $Ku(p\omega_2')^{1/p} = Ku(\alpha\omega_2')$, we see that $T' \circ I' \circ T$ is the other part of X_p.

The following lemma is the elementary case of the compatibility of Chow's construction of Jacobian varieties [2] and specialization, which we proved some time ago [7-I, Theorem 3].

LEMMA 5. *Let $\mathfrak{o}$ be a discrete valuation ring and let k be its field of fractions. Let Γ be a non-singular projective curve defined over k such that its reduction Γ' with respect to the prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ is again non-singular. Then the reduction J' of the Chow Jacobian variety J of Γ with respect to $\mathfrak{p}$ is the Chow Jacobian variety of Γ'.*

Once we have these two lemmas, by a rather simple argument [4, 12], we can incorporate Weil's results [15, 16] on the eigen values of I operating on the l-primary part of the group of points of finite orders of the Jacobian variety of C_p for a prime number l different from p, and we get the following definitive result:

THEOREM 3. *Let δX be the contravariant map of the vector space of differentials of the first kind on C induced by a modular correspondence X of a prime degree p. Then the eigen values of δX are complex numbers of absolute value at most equal to $2 \cdot p^{\frac{1}{2}}$.*

We note that there is one non-algebraic theorem creeping in the above mentioned "simple argument." In fact, the relation between the representations of the correspondence X on the vector space of differentials of the first kind on C and on the l-primary part of the group of points of finite orders of the Jacobian variety of C can be proved, at least at present, only with the aid of Riemann's transcendental theory.

5. Cusp forms. In this last section, we shall formulate the Petersson conjecture and we shall show that it is solved for dimension -2. Suppose that C is the curve constructed in Section 2. Then any symmetric w-fold differential on C will be called a *modular form* of *dimension* $-2w$ and of *level* n. Here w is, of course, a non-negative integer. It is clear that a modular form can be written uniquely in the form $f(dj)^w$ with some function f on C. A modular form of dimension zero is called a *modular function.* Actually, if we uniformize the curve C by a transcendental parameter z which is a variable in the upper half-plane, the analytic function $f(dj/dz)^w$ is the classical modular form [cf. 6-I]. At any rate, the modular correspondence X of degree m introduced in the previous section gives rise to a contravariant map $T(m)$ of the space of modular forms to itself. The operator $T(m)$ so defined can be called the *Hecke operator* although Hecke put the weight factor m^{w-1} [6-II]. We shall now introduce cusp forms but after this general remark:

Suppose that r is a positive integer and let C^* be the curve in Section 2 for the level rn. Then, the multiplication by r of the elliptic curve A_j defined before induces a unique projection from C^* to C, which is a rational mapping defined over Q. Moreover, if m is relatively prime to r and if X^* is the modular correspondence of degree m and of level rn, the following diagram is commutative:

$$\begin{tikzcd} C^* \arrow[r, "X^*"] \arrow[d, "r"] & C^* \arrow[d, "r"] \\ C \arrow[r, "X"] & C. \end{tikzcd}$$

The verification is immediate. An attentive reader might have noticed that a similar diagram was used already in the proof of Lemma 4. We note also that in case r is relatively prime to n, the same procedure as above gives rise to a birational correspondence Y of C to itself. If $R(r)$ is the corresponding contravariant map of the space of modular forms, the following multiplication formula comes out rather formally:

$$T(m)\cdot T(m') = \sum_{d|m,m'} d\cdot R(d)\cdot T(mm'/d^2).$$

A modular form $f(dj)^w$ is called a *cusp form* if the corresponding classical modular form $f(dj/dz)^w$ is holomorphic everywhere in the upper half-plane and vanishes at "cusps." As we can see without difficulty, it is the same thing to say that $f(dj)^w$ becomes a modular form of the first kind, i. e. a modular form without poles, on C^* for $r=w$. In particular, a cusp form of dimension -2 and a differential of the first kind are the same thing. At any rate, the space of cusp forms of dimension $-2w$ on C can be identified with a subspace of the space of modular forms of the first kind on C^* for $r=w$. The number of independent cusp forms of a fixed dimension is, therefore, finite and it can be calculated very easily by the Riemann-Roch theorem.

Now in [10] Petersson conjectured that for a subspace of the space of cusp forms of a fixed dimension which is stable under Hecke operators the eigen values of $T(p)$ are complex numbers of absolute value at most equal to $2\cdot p^{\frac{1}{2}}$. It is clear from the above explanation that Theorem 3 solves this conjecture completely for dimension -2. In the case of level one, if we observe that C^* for $r=6$ is the first curve with positive genus, we see that the first cusp form is of dimenstion -12. Moreover, since we have seen that C^* for $r=6$ is an equianharmonic elliptic curve, there exists only one cusp form for dimension -12 and it can be expressed as $(dx/y)^6$ on $y^2=x^3-1$. This expression might be helpful for the investigation of the Petersson conjecture in this case, which was raised by Ramanujan.

In concluding this paper, we note that the theory of Hecke operators can be discussed geometrically along our development. We can introduce *integral forms* to be those modular forms which become of the first kind so-to-speak on the limit of C^* for $r\to\infty$. Actually, we can very easily write down the condition and the Riemann-Roch theorem permits us to compute the number of independent integral forms of a fixed dimension. Also, we can prove its stability under $T(m)$, etc. However, we shall leave it as an exercise to the reader.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] W. L. Chow, "On the genus of curves of an algebraic system," *Transactions of the American Mathematical Society*, vol. 65 (1949), pp. 137-140.

[2] ———, "The Jacobian variety of an algebraic curve," *American Journal of Mathematics*, vol. 76 (1954), pp. 453-476.

[3] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität*, vol. 14 (1941), pp. 197-272.

[4] M. Eichler, "Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion," *Archiv der Mathematik*, vol. 5 (1954), pp. 355-366.

[5] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper," I, *Journal für die reine und angewandte Mathematik*, vol. 175 (1936), pp. 55-62.

[6] E. Hecke, "Ueber Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung," I, *Mathematische Annalen*, vol. 114 (1937), pp. 1-28; II, *ibid.*, pp. 316-351.

[7] J. Igusa, "Fibre systems of Jacobian varieties," I, *American Journal of Mathematics*, vol. 78 (1956), pp. 171-199; III, *ibid.*, vol. 81 (1959), pp. 453-476.

[8] ———, "On the transformation theory of elliptic functions," *American Journal of Mathematics*, vol. 81 (1959), pp. 436-452.

[9] M. Nagata, "A general theory of algebraic geometry over Dedekind domains," I, *American Journal of Mathematics*, vol. 78 (1956), pp. 78-116.

[10] H. Petersson, "Konstruktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung," II, *Mathematische Annalen*, vol. 117 (1940-41), pp. 39-64.

[11] G. Shimura, "Reduction of algebraic varieties with respect to a discrete valuation of the basic field," *American Journal of Mathematics*, vol. 77 (7955), pp. 134-176.

[12] ———, "Correspondences modulaires et les fonctions ζ de courbes algébriques," *Journal of the Mathematical Society of Japan*, vol. 10 (1958),, pp. 1-28.

[13] B. L. van der Waerden, "Projective und birationale Aequivalenz und Moduln von ebenen Kurven," *Mathematische Annalen*, vol. 114 (1937), pp. 683-699.

[14] H. Weber, *Lehrbuch der Algebra*, III, Braunschweig, 1908.

[15] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Paris, 1948.

[16] ———, *Variétés Abéliennes et courbes algébriques*, Paris, 1948.

[17] O. Zariski, "Some results in the arithmetic theory of algebraic varieties," *American Journal of Mathematics*, vol. 61 (1939), pp. 249-294.

[18] ——— and P. Samuel, *Commutative algebra*, New York, 1958.

THE STRUCTURE OF LOCAL HOMEOMORPHISMS, III.*[1]

By SHLOMO STERNBERG.

In memory of Aurel Wintner.

In this paper, we continue the study of local homeomorphisms in Euclidean n-space begun in [13] and [14]. The main result to be proved here is that any C^∞ volume preserving transformation defined in some neighborhood of the origin, keeping the origin fixed, whose Jacobian matrix at the origin satisfies a formal condition (**) to be given below, can be brought by a volume preserving change of coordinates to a certain normal form. The set of germs of these normal forms fall into a finite number of classes, each of which constitutes a maximal commutative subgroup of the group of local C^∞ volume preserving maps. Furthermore, the condition (**) will be interpreted as a regularity condition. Thus, we will establish for the group of local C^∞ volume preserving maps a theorem analogous to the one which asserts that any regular element of a real Lie group is conjugate to an element of one of a finite number of Cartan subgroups. A similar analogue for the group of all local C^∞ homeomorphisms was proved in [14]. We shall also prove this result for the group of all local C^∞ maps which preserve volume up to a constant factor, and obtain partial results in this direction for the group for all local C^∞ Hamiltonian maps. Since according to Cartan [4] these are (the local versions of) three of the six primitive infinite groups, it is to be hoped that a general theory of the structure of the infinite Lie groups can be developed. The theorem proved here for the group of local volume preserving maps is the C^∞ and n-dimensional version of a theorem first proved by Moser [9] in the two dimensional analytic case; of also [11].

The 'infinite groups' of Lie and Cartan are not groups in the present day sense. They are families of homeomorphisms defined on various domains of a manifold and satisfying certain partial differential equations. They are closed under the operations of composition and taking inverses whenever

* Received March 17, 1958.

[1] This research was supported in part by the United States Air Force under contract no. AF49(638)-382 with the AF Office of Scientific Research.

these operations are defined. The trouble is, of course, that in general, the domains of definition of different homeomorphisms don't match, so they don't form a group. For modern development in the theory of these 'infinite groups' in the large and its application to the problem of equivalence in differential geometry cf. Liberman [8] and Chern [5] and the references cited there. For the foundations of the local theory, cf. Kuranishi [7]. The papers of Kuranishi and Liberman deal only with analytic transformations. The reason for this is that these papers, following Cartan, make essential use of the theory of exterior differential equations; the fundamental existence theorem in the theory of exterior differential equations depends on the Cauchy-Kowalewski theorem. The objects that we have been considering are groups since we consider only transformations leaving the origin fixed, and we identify two transformations if they agree in some neighborhood of the origin; that is, we consider the groups of germs of transformations. In this set-up, in certain respects (mainly the lack of convergence difficulties) the C^∞ case is simpler than the analytic case whereas in other respects the reverse is true. We hope to deal with the analytic case in future publications. Another way to obtain a group is to require that the domain and range of all transformations be a whole manifold. The problems involved in the study of algebraic structure of these groups seem to be quite difficult. Even in the one-dimensional case of homeomorphisms of a circle onto itself, fairly deep diophantine considerations enter, cf. Finzi [6]. These diophantine considerations (in the form of small divisors) also occur in the local analytic theory. It should be observed that the "Poincaré circle problem" is also one of establishing a conjugacy theorem. Here the group is that of all orientation preserving analytic (C^∞) homeomorphisms of the circle onto itself and the group of rotations is a maximal commutative subgroup playing the role of the Cartan subgroup. The problem of determining the correct regularity conditions and proving a conjugacy theorem remains open. It is possible that this problem is a prototype of the study of the algebraic structure of the global infinite Lie groups.

In § 1 of this paper we prove some preparatory lemmas constructing certain maximal abelian subgroups of the group of local C^∞ volume preserving maps and state the main theorem for this group. In § 2 we make a very elementary study of the structure of the algebras of all formal vector fields and formal vector fields with divergence 0. This is done to define the formal conditions (*) and (**) and show that they correspond by analogy to regularity conditions in a Lie group. In § 3 we prove the formal version of the main theorem. The proof given here is a straightforward generalization to n

dimensions of the proof for $n=2$ given in Siegel [11], pp. 135-142. In future publications we shall present a more systematic theory of groups of formal power series transformations and vector fields. The conjugacy theorem proved in § 3 for the formal volume preserving transformations and again in § 9 for the Hamiltonian group will turn out to be special cases of a general theorem on groups of formal power series transformations. We include the proofs given here for these special cases, however, because of their elementary character.

In § 4 we bring every volume preserving transformation satisfying (**) to a preliminary normal form. In § 5 we prove the following theorem. If N and T are two C^∞ homeomorphisms having the same Taylor expansions at the origin and such that no eigenvalue of the Jacobian matrix at the origin is of absolute value 1, then there exists a C^∞ homeomorphism D such as $DTD^{-1}=N$. This theorem, which is essentially the content of Theorem 3 of [14] is reproved here in greater detail because of some additional normalizations, which are necessary for the rest of the argument, on the transformation D. In § 6 we show that every local volume preserving homeomorphism satisfying (**) lies on a one-parameter group. In § 7 we conclude the proof of the conjugacy theorem for the group of local volume preserving maps. In § 8 we prove the corresponding theorem for the group of local maps which preserve volume up to a constant factor. In § 9 we prove a partial result in this direction for the group of Hamiltonian maps.

In what follows, we shall, for the sake of simplicity only consider one of the Cartan subgroups. That is, we will act as if the matrices that arise are real diagonizable, i. e. that the eigenvalues are real. However, all the arguments carry over with the obvious changes to the case of complex eigenvalues. Thus, an expression of the form $x_1x_2\cdots x_n$, might mean $(x_1^2+x_2^2)x_3\cdots x_n$ or $(x_1^2+x_2^2)(x_3^2+x_4^2)\cdots x_n$, etc., depending on how many (pairs of) complex eigenvalues occur. In order not to clutter up the language too much, we frequently do not distinguished between the germ of a transformation and a transformation defined in a sufficiently small neighborhood. The reader is also advised to liberally sprinkle the phrase 'in a sufficiently small neighborhood of' throughout the paper. This paper depends fairly heavily on the results of [13] and the ideas of [14]. It can be read independently of [14], but not of [13].

1. Before proceeding to the statement of the theorem let us briefly resume and place in a more algebraic setting the results of [14]. Let $\boldsymbol{G}^n$

denote the group of all local C^∞ maps. Then the set of all (complex) diagonal linear transformations of $\boldsymbol{G}^n$, i.e., transformations of the form

$$x_i^* = \lambda_i x_i \tag{i}$$

constitute a commutative subgroup of $\boldsymbol{G}^n$. (It is to be understood that (i) is a real transformation. If a complex eigenvalue, λ_i, occurs in (i) then so will $\bar{\lambda}_i$ and the resulting pair of equations in (i) represents the corresponding rotation-dilatation in the appropriate two dimensional space. This and/or a similar convention will be followed throughout this paper.) We observe that the transformations (i) actually form a maximal commutative subgroup of $\boldsymbol{G}^n$. In fact, if T commutes with all of (i), then since projection onto the Jacobian matrix is a homomorphism and the (i) form a maximal commutative subgroup of the general linear group, the linear terms of T must be of the form (i). Thus T can be written in the form

$$x_i^* = \mu_i x_i + \phi_i(x_1, \cdots, x_n), \tag{ii}$$

with $\phi_i(0, \cdots, 0) = O(v^2)$. The condition that T commutes with all of (i) implies that $\lambda_i^{-1}(\lambda_1 x_1, \cdots, \lambda_n x_n) = \phi_i(x_1, \cdots, x_n)$ for all non-vanishing λ's. Letting the λ's tend to zero shows that $\phi_i = 0$. The main theorem cf [10] asserts that if S is an element of $\boldsymbol{G}^n$ whose matrix of linear terms is equivalent to a transformation of the form (i) and such that

$$\lambda_i \neq \lambda_1^{m_1} \cdots \lambda_n^{m_n} \qquad (m_j \text{ non-negative integers with } \textstyle\sum m_i > 1), \tag{*}$$

then S is conjugate via an inner automorphism of $\boldsymbol{G}^n$ to an element of (i). We shall discuss condition (*) further in § 2.

Now let $\boldsymbol{V}^n$ denote the group of all volume preserving maps. Here, the projection onto linear terms maps $\boldsymbol{V}^n$ onto the special linear map. A maximal commutative subgroup of the special linear group is the set of all transformations of the form

$$x_i^* = \lambda_i x_i \text{ with } \textstyle\prod \lambda_i = 1. \tag{1}$$

The transformations (1) do not, however, form a maximal commutative subgroup of $\boldsymbol{V}^n$. In fact, any transformation of the form (1) clearly commutes with any transformation of the form

$$x_i^* = x_i f_i(x_1 x_2 \cdots x_n)\,; \tag{2}$$

Here the f_i are functions of one variable, the product $x_1 \cdots x_n$. It is easy to see that any transformation T of $\boldsymbol{V}^n$ commuting with all of (1) must be of the form (2); by the same argument as before, T has the form (ii) with

$\prod \mu_i = 1$. Now if $\phi_i = x_i\psi_i + \eta_i(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots x_n)$, then, letting the $\lambda_j \neq \lambda_i$ approach 0, we can conclude that $\eta_i = 0$ and $\psi_i(\lambda_1 x_1, \cdots, \lambda_n x_n) = \psi_i(x_1, \cdots, x_n) =$ for all λ_i such that $\prod \lambda_i = 1$. If one of the x_i's vanishes we can apply the previous argument so that the $\psi_i = 0$ along the hyperplanes $x_j = 0$. If none of the x_i vanishes and $x_1 \cdots x_n = y_1 \cdots y_n$, then taking $\lambda_i = y_i/x_i$ we have $\psi_i(x_1, \cdots, x_n) = \psi_i(y_1, \cdots, y_n)$. Thus T has the form (2).

Of course, not all transformations of the form (2) belong V^n. In order to determine which ones do, we need

LEMMA 1. *Let T be a transformation of the form (2) and let $\omega = x_1 \cdots, x_n$. Then the Jacobian of T is $d/d\omega(\omega \prod f_i(\omega))$.*

Proof. A direct computation shows that the transformation S given by

$$\begin{aligned} x_i^* &= x_i & (i = 1, \cdots, n-2), \\ x_{n-1}^* &= x_{n-1} f_n(\omega), \\ x_n^* &= x_n / f_n(\omega) \end{aligned} \tag{3}$$

is volume preserving. The transformation TS has the same Jacobian as T and has the form

$$\begin{aligned} x_i^* &= x_i f_i(\omega) & (i = 1, \cdots, n-2), \\ x_{n-1}^* &= x_{n-1} f_{n-1}(\omega) f_n(\omega), \\ x_n^* &= x_n. \end{aligned} \tag{4}$$

Continuing in this manner, we finally arrive at a transformation given by

$$\begin{aligned} x_1^* &= x_1 \prod f_i(\omega), \\ x_i^* &= x_i & (i > 1). \end{aligned} \tag{5}$$

A direct computation of the Jacobian of (5) proves the lemma.

In particular, setting $h(\omega) = \prod f_i(\omega)$, if T is to be a volume preserving transformation, h must satisfy the differential equation $\omega h'(\omega) + h(\omega) = 1$. If h is to be regular at the origin, we must have $h = 1$. Since all transformations (2) with $h = 1$ commute with one another and the inverse of (2) is again of that form, we have proved

LEMMA 2. *The set of all transformations of the form (2) with $\prod f_i = 1$ is a maximal commutative subgroup of V^n. We will denote this subgroup by $\mathfrak{C}^n$.*

If we examine the formal condition (*), we see that it is violated for

every element of V^n since $\prod \lambda_i = 1$. By Theorem 3 of [14], if (for a transformation $T \in V^n$) this is the only violation of (*), there exists a C^∞ change of coordinates R such that RTR^{-1} is of the form (2). The purpose of this paper is to show that R can be chosen to be volume preserving so that (automatically) RTR^{-1} is an element of C^n. Thus we wish to prove

THEOREM 1. *Let $T \in V^n$, $n > 2$, have a (complex) diagonizable linear part whose eigenvalues, $\lambda_1, \cdots, \lambda_n$, satisfy*

$$(**) \qquad \text{if } \lambda_i = \lambda_1^{m_1} \cdots \lambda_n^{m_n}, \text{ then } m_i - 1 = m_j \text{ for all } j \neq i,$$

then there exists an $R \in V^n$ such that $RTR^{-1} = N \in C^n$. For the case $n = 2$, the above statement is true under the additional hypothesis $|\lambda_i| \neq 1$.

Remark. In the case $n > 2$, the condition $\lambda_i \neq 1$ is a consequence of (**).

2. In this section, which will not be needed for what follows, we shall try to give some meaning to conditions (*) and (**). We do this by examining the root structure of the Lie algebras of all formal fields and formal vector fields with divergence zero. In future publications we shall examine the connection between groups of formal power series transformations and Lie algebras of formal vector fields and obtain a structure and representation theory for such algebras. For the present, our justification of (*) and (**) will merely be by analogy to the case of a finite dimensional Lie group.

By a formal vector field, f, we shall mean a vector $f = (u_1 \cdots u_n)$ where each of the u_i is a formal power series in $x_1, \cdots, x_n$ with no constant terms. For simplicity, we shall allow complex coefficients. By the Lie bracket $[g, f]$, with $g = (v_1 \cdots v_n)$, we shall mean the formal vector field $h = (w_1, \cdots, w_n)$, where the w_i are given by

$$(6) \qquad w_i = \sum_j (u_j \partial v_i / \partial x_j - v_j \partial u_i / \partial x_j).$$

Let g^n denote the collection of all formal vector fields and let v^n denote those vector fields $f = (u_1, \cdots, u_n)$ such that $\sum \partial u_i / \partial x_i = 0$. Then it is clear that g^n and v^n are (infinite dimensional) Lie algebras. Let us first examine the algebra g^n. The set of diagonal linear vector fields, l^n, forms a commutative subalgebra. Let $l = (\lambda_1 x_1, \cdots, \lambda_n x_n)$ be an element of l^n and let $f = (u_1, \cdots, u_n)$ be in g^n, where

$$(7) \qquad u_i = \sum a^i_{j_1 \cdots j_n} x_1^{j_1} \cdots x_n^{j_n}.$$

Then $[l, f] = (w_1, \cdots, w_n)$, where the w are given by

$$w_i = \sum (\lambda_i - j_1\lambda_1 \cdots - j_n) a^i_{j_1 \cdots j_n} x_1^{j_1} \cdots x_n^{j_n}. \tag{8}$$

From (8) it follows immediately that l^n is a maximal abelian subalgebra of g^n. Furthermore, the linear forms $\lambda_i - \sum m_j \lambda_j$ (m_j non-negative integers with $\sum m_i \geqq 1$) form a system of roots on this commutative subalgebra. The corresponding root vectors are the vector fields $r = (r_1, \cdots, r_n)$, where $r_k = a^k x_1^{n_{k1}} x_2^{n_{k2}} \cdots x_n^{n_{kn}}$ and the integers n_{k_l} satisfy $n_{k_l} - \delta_k{}^l = m_l - \delta_i{}^l$. Here it is to be understood that if no non-negative n_k with $\sum n_{k_l} > 1$ can be found, the term r_k is to be taken as zero.

Thus the condition (*) is the straightforward generalization of the regularity condition for an element in a semi-simple Lie group. (The reason that in (*) we require $\sum m_i > 1$ instead of $\sum m_i \geqq 1$ is that in the hypothesis of Theorem 1 of [10] we assume that the linear terms of the transformation is diagonizable.) Thus Theorem 1 of [10] asserts that any regular element of G^n is conjugate to an element of the "Cartan subgroup" of diagonal linear transformations.

In the algebra $\boldsymbol{v}^n$ the diagonal linear vector fields of trace zero form a commutative subalgebra. The linear forms $\lambda_i - \sum m_j \lambda_j$ except for those where $m_j - \delta_j{}^i = m$, form a system of roots. The vector fields of the form $(r_1, \cdots, r_n)$, where the $r_i = x_i f_i(\omega)$ and $\sum f_i = 0$, form a maximal commutative subalgebra. Theorem 1 thus asserts (at least for $n > 2$) that every regular element of $\boldsymbol{V}^n$ is conjugate to an element of the Cartan subgroup $\boldsymbol{C}^n$.

3. In this section we prove the formal analogue of Theorem 1. The proof is a straightforward generalization of the classical two-dimensional case, cf. Siegel [7].

THEOREM 2. *Let $\mathfrak{G}^n$ denote the group of formal volume preserving transformations and $\mathfrak{C}^n$ the formal transformations of the form* (2), *where* $\prod f_i(\omega) = 1$. *Then if $T \in \mathfrak{G}^n$ satisfies* (**), *there exists an $R \in \mathfrak{G}^n$ such that*

$$RN = TR, \quad \textit{where } N \in \mathfrak{C}^n. \tag{9}$$

Proof. By a preliminary linear change of variables we can assume that the linear part of T is a diagonal form. We shall then look for an R whose linear part is the identity matrix. Then if $T = (t_1, \cdots, t_n)$, where

$$t_i = \lambda_i x_i + \sum_{(j_1 + \cdots + j_n > 1)} t^i_{j_1 \cdots j_n} x_1^{j_1} \cdots x_n^{j_n}, \tag{10}$$

we wish to find an $R = (r_1, \cdots, r_n)$ with

$$r_i = x_i + \sum_{(j_1+\cdots+j_n>1)} r^i{}_{j_1\cdots j_n} x_1{}^{j_1}\cdots x_n{}^{j_n} \tag{11}$$

and an $N = (x_1 f_1(\omega), \cdots, x_n f_n(\omega))$, where the f_i are given by

$$f_i = \sum_{l=0}^{\infty} f^i{}_l \omega^l = \sum_{l=0}^{\infty} f^i{}_{ll\cdots l} x_1{}^l \cdots x_n{}^l. \tag{12}$$

(Let us repeat that we are proceeding as if the eigenvalues λ_i are real. The transition to complex eigenvalues can be made either by passing to the complex field and then observing that all the formal power series that arise satisfy a reality condition as was done in [13], cf. also [3] and [10]; or by staying within the real field and making only trivial modifications of the arguments below.)

We now follow § 4 of [13]. Given a lattice vector $(\alpha_1, \cdots, \alpha_n)$, we define its height k to be $\sum \alpha_k$. Then, substituting (10), (11) and (12) into (9) and comparing the coefficients of $x_1{}^{\alpha_1}\cdots x_n{}^{\alpha_n}$, we obtain

$$r^i{}_{\alpha_1\cdots\alpha_n} \lambda_1{}^{\alpha_1}\cdots\lambda_n{}^{\alpha_n} + f^i{}_{ll\cdots l} + P_1 = \lambda_i r^i{}_{\alpha_1\cdots\alpha_n} \tag{13}$$

if $\alpha_k - \delta_i{}^k = l$. In all other cases we obtain

$$r^i{}_{\alpha_1\cdots\alpha_n} \lambda_1{}^{\alpha_1}\cdots\lambda_n{}^{\alpha_n} + P_1 = \lambda_i r^i{}_{\alpha_1\cdots\alpha_n} + P_2. \tag{14}$$

In both equations (13) and (14) the P's represent polynomials in $r^j{}_{\beta_1\cdots\beta_n}$ and $f^j{}_{p\cdots p}$, where the $(\beta_1, \cdots, \beta_n)$ and $(p, \cdots, p)$ are all of height less than k. Thus, if the case (14) applies, $r^i{}_{\alpha_1\cdots\alpha_n}$ is uniquely determined by the $r^j{}_{\beta_1\cdots\beta_n}$ and $f^j{}_{p\cdots p}$ of lower height by virtue of condition (**). If the case of (13) applies, no condition at all is imposed on $r^i{}_{\alpha_1\cdots\alpha_n}$ (since $\prod \lambda_i = 1$), whereas the $f^i{}_{l\cdots l}$ is determined by the terms of lower height. If we were to choose the $r^i{}_{\alpha_1\cdots\alpha_n}$ corresponding to the case (13) arbitrarily, we would have an R of the form (11) and an N of the form (12) which satisfy (9). However, this will not do for Theorem 2 since we want: a) R to be volume preserving and b) $\prod f_i = 1$. Now b) is a consequence of a) by (the formal analogue of) Lemma 2. Thus we must show that it is possible to choose the $r^i{}_{\alpha_1\cdots\alpha_n}$ at our disposal in such a way that

$$\Delta(x_1, \cdots, x_n) = |\,\partial r^i/\partial x^j\,| = 1. \tag{15}$$

We do this by making the following choice of $r^i{}_{\alpha_1\cdots\alpha_n}$: Choose the $r^i{}_{\alpha_1\cdots\alpha_n}$, where $\alpha_j - \delta_i{}^j = q$, so that

$(16)_q$ $\quad \Delta - 1$ contains no term of the form ω^p with $p \leqq q$.

We first show that a choice is possible. For the case $q = 0$, this condition is

trivial. Now in the power series expansion of Δ the coefficient of ω^q is a polynomial in those $r^i{}_{\alpha_1\cdots\alpha_n}$ of height at most $nq+1$. Thus if $(16)_q$ is satisfied for $q<l$, then we must choose the $r^i{}_{\alpha_1\cdots\alpha_n}$, where $\alpha_j-\delta_i{}^j=l$, so that in the formal power series expansion of $\Delta-1$ the coefficient of ω^l is 0. Remembering that the linear part of R is the identity matrix, we obtain that the coefficient of ω^l is

$$(17) \qquad r^1{}_{l+1,l\cdots l}+\cdots+r^n{}_{l\cdots l,l+1}+Q,$$

where Q is a polynomial in terms of height $\leqq nl$. Thus the condition $(16)_q$ reduces to a single linear equation for the $r^i{}_{\alpha_1\cdots\alpha_n}$ and so can be satisfied.

We now choose the $r^i{}_{\alpha_1\cdots\alpha_n}$ with $\alpha_j-\delta_i{}^j=q$ arbitrarily, subject to the condition $(16)_q$. Then R and N are uniquely determined by (13) and (14). Furthermore, $\Delta-1$ contains no term in ω. We wish to show that (15) is satisfied. Now since $RN=TR$ and N is of the form (2), we have

$$(18) \qquad \Delta(x_1f_1,\cdots,x_nf_n)\,d/d\omega[\omega\prod f_i(\omega)])=\Delta(x_1,\cdots,x_n)$$

since T is volume preserving and the Jacobian of N is given by (the formal analogue of) Lemma 1. If we set

$$\Gamma(x_1,\cdots,x_n)=\sum\gamma_{\alpha_1\cdots\alpha_n}x_1{}^{\alpha_1}\cdots x_n{}^{\alpha_n}=\Delta(x_1\cdots x_n)-1$$

and

$$h(\omega)=\sum h_{ll\cdots l}x_1{}^l\cdots x_n{}^l=d/d\omega[\omega\prod f_i(\omega)]-1,$$

then $\Gamma(0,\cdots,0)=h(0)=0$. We wish to prove that Γ and h vanish identically. In terms of Γ and h, (18) becomes

$$(19) \qquad \Gamma(x_1f_1,\cdots,x_nf_n)+h(\omega)+\Gamma(x_1f_1,\cdots,x_nf_n)h(\omega)=\Gamma(x_1,\cdots,x_n).$$

We have chosen R so that the $\gamma_{ll\cdots l}=0$. We prove that the remaining $\gamma_{\alpha_1\cdots\alpha_n}$ and $h_{ll\cdots l}$ vanish by induction on their height. As we have seen, the terms of height 0 vanish. We thus assume that all terms of height $k-1$ vanish. If $(\alpha_1,\cdots,\alpha_n)$ is of height k and is not of the form $(l,l,\cdots,l)$, then comparing the coefficients of $x_1{}^{\alpha_1}\cdots x_n{}^{\alpha_n}$ in (19), we obtain (since $f^i{}_{00\cdots 0}=\lambda_i$)

$$\gamma_{\alpha_1\cdots\alpha_n}\lambda_1{}^{\alpha_1}\cdots\lambda_n{}^{\alpha_n}+Q=\gamma_{\alpha_1\cdots\alpha_n},$$

where Q is a polynomial with no constant terms in the terms of lower height; thus $Q=0$. Then, by (**), $\gamma_{\alpha_1\cdots\alpha_n}=0$. Comparing the coefficients of $x_1{}^lx_2{}^l\cdots x_n{}^l$, we obtain, since $\gamma_{ll\cdots l}=0$, that $h_{ll\cdots l}$ is a polynomial in the lower order terms. Thus $h_{ll\cdots l}=0$. This completes the proof of Theorem 2.

4. In this section we show how to bring every volume preserving transformation to a preliminary normal form. For this purpose we need the analogue of Lemma 5 of [10].

LEMMA 3. *Let $S = (s_1, \cdots, s_n)$ be a formal volume preserving transformation whose linear part is the identity matrix. Then there exists a C^∞ volume preserving transformation $S = (s_1, \cdots, s_n)$, where s_i is the Taylor series expansion of s_i.*

Proof. Choose $s_1, \cdots, s_{n-1}$ arbitrarily as C^∞ functions whose Taylor series is $s_1, \cdots, s_{n-1}$. (This can be done by Lemma 5 of [10].) Let s_{n0} denote the formal power series in $n-1$ variables obtained from s_n by setting $x_n = 0$, and let s_{n0} denote a C^∞ function defined on the hyperplane $x_n = 0$, and whose Taylor series expansion is s_{n0}. Then the linear partial differential equation $| \partial s_i / \partial x_j | = 1$ for s_n is non-characteristic on the hyperplane $x_n = 0$. On this hyperplane we assign the initial values $s_n(0) = s_{n0}$. Then the solution s_n is a C^∞ function which, together with $s_1, \cdots, s_{n-1}$, gives a volume preserving transformation S. Since the corresponding formal partial differential equation has the unique solution s_n, the Taylor series of s_n is s_n, proving the lemma. If S is of the form (2), then we can prove the lemma more directly and still retain the form (2). In fact, if $s_i = x_i f_i(\omega)$, then choose the first $n-1$ C^∞ functions f_i of one variable ω and set $f_n = 1/f_1 \cdots f_{n-1}$.

Using Theorem 2 and Lemma 3, we obtain

LEMMA 4. *Let T be an element of $\mathbf{V}^n$ satisfying (**). Then there exists an $N \in \mathbf{C}^n$ and a volume preserving change of coordinates so that in the new coordinate system $T - N$ vanishes at the origin with infinite order.*

Now since no $|\lambda_i| = 1$, we can assume that the $|\lambda_i|$ are ordered so that

$$|\lambda_1| \leqq \cdots \leqq |\lambda_k| < 1 < |\lambda_{k+1}| \leqq \cdots \leqq |\lambda_n|.$$

As in [10], we introduce the norms

$$\| x \|_+ = \sum_1^k x_i^2, \qquad \| x \|_- = \sum_{k+1}^n x_i^2, \qquad \| x \| = \| x \|_+ + \| x \|_-$$

and the

$$S_+ = \{x \mid \| x \|_+ < \| x \|_-\}, \qquad S_- = \{x \mid \| x \|_+ > \| x \|_-\},$$

$$I_+ = \{x \mid \| x \|_+ = 0\},\ C = \{x \mid \| x \|_+ = \| x \|_-\} \text{ and } I_- = \{x \mid \| x \|_- = 0\}.$$

Now the spaces I_+ and I_- are invariant under N, and N is an expansion (contraction) on I_+ (I_-). By Theorem 7 of [13], there exist two invariant surfaces under T,

$$J_+ : x_i = \phi_i(x_{k+1}, \cdots, x_n) \qquad (i = 1, \cdots, k),$$

$$J_- : x_j = \phi_j(x_1, \cdots, x_k) \qquad (j = k+1, \cdots, n),$$

where the ϕ_i are C^∞ and vanish at the origin with infinite order. Now the transformation

$$x^*_i = x_i - \phi_i(x_{k+1}, \cdots, x_n) \text{ for } i \leqq k, \; x^*_i = x_i \text{ for } i > k$$

is clearly volume preserving and is the identity at the origin up to terms of infinite order. In the x^* coordinate system the surface J_+ coincides with I_+ and J_- has the form

$$x^*_j = \eta_j(x^*_1, \cdots, x^*_k), \qquad j > k,$$

where the η vanish with infinite order at the origin. Then the transformation

$$x^{**}_1 = x^*_i \text{ for } i \leqq k, \qquad x^{**}_j = x^*_j - \eta_j(x^*_1, \cdots, x^*_k) \text{ for } j > k$$

leaves I_+ invariant and takes J_- into I_-. We thus can choose an $M \in \boldsymbol{V}^n$ so that the invariant surfaces of MTM^{-1} and N are I_+ and I_-. The new T and N are expansions on I_+ which coincide up to terms of infinite order of the origin. We can, by Theorem 2 of [9], find a C^∞ transformation X defined on the space I_+ so that

$$XT_{I_+}X^{-1} = N_{I_+}.$$

If x_+ and x_- denote the projections of x onto I_+ and I_- respectively, we then defined a transformation Q in a neighborhood of the origin by

$$x^*_+ = Xx_+, \qquad x^*_- = (\det X(x_+))^{-1/(n-k)}x_-.$$

Then $Q \in \boldsymbol{V}^n$, the restriction of Q to I_- is the identity and $Q - E$ vanishes at the origin with infinite order, where E is the identity transformation. After transforming by Q, the transformations T and N coincide on I_+. Doing the same for I_-, we obtain

LEMMA 5. *Let $T \in \boldsymbol{V}^n$ satisfy (**). Then there exist an $N \in \boldsymbol{C}^n$ and an $S \in \boldsymbol{V}^n$ so that $STS^{-1} - N$ vanishes along I_+ and I_- and vanishes at the origin with infinite order.*

5. In this section, we shall construct a $D \in \boldsymbol{G}^n$ so that

$$DT = ND. \tag{20}$$

This is a consequence of Theorem 3 of [14]. However, since no details of the proof are given there, we shall reprove this theorem here. For a sketch of and a motivation for the arguments of this section cf. [14], pp. 624-625.

We shall assume for convenience that N has been extended to all space so as to remain a C^∞ transformation (not necessarily a homeomorphism) and

so that its derivatives of every order remain bounded. We choose a ball B_ρ: $\| x \| \leqq \rho$ so small that $\| (T-L)x \|_\pm < \epsilon \| x \|_\pm$, where L is the linear part of T, which we can do since I_+ and I_- are invariant. Then $T(B_\rho \cap S_+) \subset S_+$ and we set, for $r < \rho/3$

$$
\begin{aligned}
& W_{0,r} = \overline{B_r \cap S_+ - T(B_\rho \cap S_+)}, \\
(21) \qquad & W_{n,r} = TW_{n-1,r} \cap B_r \text{ for } n > 0, \text{ and} \\
& W_{n,r} = T^{-1}W_{n+1,r} \cap B_r \text{ for } n < 0.
\end{aligned}
$$

It is then clear as in the proof of Lemma 2 of [10], that

$$
(22) \qquad B_{r/3} \subset I_+ \cup I_- \cup \bigcup_{n=-\infty}^{\infty} W_n.
$$

We define the transformation D in $W = W_{0,r}$ as follows: we set $D =$ identity on C and (for later purposes) in a neighborhood in W of every point of C different from the origin, where at each point we choose a neighborhood so small that it does not intersect TC. This then defines D on TC by (20). That is, at a point $x = Ty$ of TC, we set $Dx = Ny$. Then, as in Lemma 8 and the paragraphs immediately following it of [14], we can "fill in" D so that $D - E$ vanishes at the origin with infinite order, where E is the identity transformation, and satifies the above requirements at the boundary of C. Now D is defined on $W_{0,r}$. We define it on all $W_{k,r/3}$ by (20). That is, for $x \in W_{k,r}$ we set $Dx = N^kDT^{-k}x$. Then D is defined everywhere in a neighborhood of the origin except on the surfaces I_+ and I_-, and is a C^∞ at these surfaces. We first show that it is continuous there. For this purpose it is sufficient to show that $D - E$ evaluated at any point of $W_{k,r/3}$ tends to zero as $|k| \to \infty$. We shall show this for $k \to +\infty$; for $k \to -\infty$ the situation is entirely analogous. We first need a slightly different version of Lemma 3 of [10].

LEMMA 6. *There exists a constant $\kappa < 1$ such that for sufficiently small r and all sufficiently large $k \geqq k_0$,*

$$
(23) \qquad T^{-1}W_{k+1,r} \subset W_{k,\kappa r}.
$$

Proof. Since I_+ and I_- are invariant we can choose r_1 so small that $\| Tx \|_- \geqq c_1 \| x \|_-$ and $\| Tx \|_+ \leqq c_2 \| x \|_+$ for all $x \in B_r$, where $c_1 > 1 > c_2$. We then choose a k_δ so large that $\| x \|_- \geqq (1-\delta) \| x \|$ for all $x \in W_{k,r}$, where $k \geqq k_\delta$, and $r \leqq r_1$. Then $\| Tx \| \geqq \| Tx \|_- \geqq c_1 \| x \|_- \geqq c_1(1-\delta) \| x \|$ for $x \in W_{k,r}$. If we choose δ so small that $c_1(1-\delta) > 1$, then setting $\kappa = 1/c_1(1-\delta)$, we have (23).

For any $l < k_0$, $\| T^k x \| \geqq \| T^l x \|_- \geqq c_1{}^k \| x \|_- \geqq \frac{1}{2} c_1{}^k \| x \|$, so that $\| x \|$ is decreased by at most a factor of $\frac{1}{2}$.

We also need an analogue of the mean value theorem.

LEMMA 7. *Let U, Y, and Z be three smooth transformations (with the proper domains of definition), $U(x) = (u_1(x_1, \cdots, x_n), \cdots, u_n(x_1, \cdots, x_n))$, etc. Then*

$$U(Z + Y) = U(Z) + U' \cdot Y, \tag{24}$$

where U' is a matrix made up of the partial derivatives $\partial u_i / \partial x_j$ evaluated at various points on the lines joining $(z_1, \cdots, z_n)$ to

$$(z_1 + y_1, \cdots, z_n), \cdots, (z_1 + y_1, \cdots, z_{n-1} + y_{n-1}, z_n)$$

to $(z_1 + y_1, \cdots, z_n + y_n)$.

Proof.

$$\begin{aligned} u_i(z_1 + y_1, \cdots, z_n + y_n) = u_i(z_1, \cdots, z_n) &+ (u_i(z_1 + y_1, \cdots, z_n) \\ - u_i(z_1, \cdots, z_n)) &+ \cdots + (u_i(z_1 + y_1, \cdots, z_n + y_n) \\ - u_i(z_1 + y_1, \cdots, z_{n-1} + y_{n-1}, z_n)). \end{aligned}$$

Then apply Taylor's formula.

If we now set

$$N = T + G \tag{25}$$

and

$$P_k = N^k D T^{-k} - E \text{ on } W_k, \tag{26}$$

then, since G and P_0 vanish at the origin with infinite order, for any q there exists a constant A_q such that

$$\| G(x) \| < A_q \| x \|^q \tag{27}$$

and

$$\| P_0(x) \| < A_q \| x \|^q. \tag{28}$$

In view of (26), we have the following recursion formula for P_k:

$$P_{k+1} = N(P_k + E) T^{-1} - E. \tag{29}$$

By repeated use of Lemma 7, we can rewrite (29) as

$$P_{k+1} = N'(E + \theta P_k) \cdot P_k T^{-1} + G T^{-1}, \tag{30}$$

where the matrix N' is the one given by Lemma 7. Thus

$$P_k = GT^{-1} + N'(E+\theta P_{k-1})GT^{-2} + N'(E+\theta P_{k-1})N'(E+\theta P_{k-2})GT^{-3} + \cdots + N'(E+\theta P_{k-1})\cdots N'(E+\theta P_0)P_0T^{-k}. \tag{31}$$

Now set

$$M = \sup_{B_r} | \partial n_i/\partial x_j | \tag{32}$$

and choose q so large that

$$\kappa^q M n = \alpha < 1. \tag{33}$$

In view of Lemma 6 and (27), for any point in $W_{k,r}$, we have

$$\sup_{W_{k,r}} \| GT^{-p}(x) \| \leqq A_q r^q \kappa^{qp}, \tag{34}$$

for $k - p \geqq k_0$, and

$$\sup_{W_{k,r}} \| GT^{-p}(x) \| \leqq A_q 2^q r^q \kappa^{q(k-k_0)} \tag{35}$$

for $k - p < k_0$. Similarly, by (28),

$$\sup_{W_{k,r}} \| P_0 T^{-k}(x) \| \leqq A_q 2^q r^q \kappa^{q(k-k_0)}. \tag{36}$$

Using (31), we have, for large values k and all m such that $k - m \geqq k_0$,

$$\| P_k \| \leqq \| GT^{-1} + N'(E+P_{k-1})GT^{-2} + \cdots + N'(E+P_{k-1})\cdots \cdots N'(E+P_{k-m})GT^{-m} \| + A_q r^q \alpha^m/(1-\alpha) + 2^q k_0 (Mn)^{k_0} A_q \alpha^{k-k_0} \tag{37}$$

Now for any ϵ, we choose m_ϵ so large that the second term on the right of (37) is $\leqq \epsilon/3$. We then take k_ϵ so large that the third term on the right $\leqq \epsilon/3$ for all $k \geqq k_\epsilon$. The remaining term on the right can be majorized by an expression of the form

$$B_2 \| GT^{-1} \| + B_2 \| GT^{-2} \| + \cdots + B_m \| GT^{-m} \|, \tag{38}$$

where the B's are constants. Now as $k \to \infty$, x approaches I_+, as do the points $T^{-1}x, \cdots, T^{-m}x$. (Remember that now m is large but *fixed*.) Since, by assumption $G(p) \to 0$ as $p \to I_+$, by choosing $k_{-\epsilon}$ sufficiently large, we can make (38) $< \epsilon/3$. We have thus proved the continuity of D at I_+.

The sequence $(1/\| x \|^h)P_m$ also converges (to zero) by the above argument. This can be seen most easily by absorbing the h into the q of (27) and (28). Thus for any h, there exists a constant A'_n such that

$$\| (D-E)x \| \leqq A'_n \| x \|^h. \tag{39}$$

In order to prove that D is C^∞ at I_+, it suffices to prove

LEMMA 8. *Let* $D - E = F = (f_1, \cdots, f_n)$. *Then if* $p \in I_+$, $p_k \notin I_+$, *and* $p_n \to p$, *the sequence* $\partial f_i(p_k)/\partial x_1^{l_1} \cdots \partial x_n^{l_n}$ *converges.*

The proof of Lemma 7 is essentially the same as the proof of the continuity of D except that the estimates are a little more complicated. In the wedge W_k, the transformation F coincides with P_k. Thus if f_i^k are the coordinate functions of P_n, (29) becomes

$$f_i^{k+1}(x) = n_i(T^{-1}x + P_k T^{-1}x) - x_i. \tag{40}$$

Differentiating (40) and setting $T^{-1} = (t^*{}_1, \cdots, t^*{}_n)$, we obtain

$$\begin{aligned}(\partial f_i^{k+1}/\partial x_j)(x) &= [\sum_{j_1} (\partial t_i/\partial x_{j_1})(T^{-1}x + P_k T^{-1}x)(\partial t^*{}_{j_1}/\partial x_j)(x) - \delta^j{}_i] \\ &+ [\sum_{j_1} (\partial q_i/\partial x_{j_1})(T^{-1}x + P_k T^{-1}x)(\partial t^*{}_{j_1}/\partial x_j)(x)] \\ &+ [\sum_{j_1, j_2} (\partial u_i/\partial x_{j_1})(T^{-1}x + P_k T^{-1}x)(\partial f^k{}_{j_1}/\partial x_{j_2})(T^{-1}x)(\partial t^*{}_{j_2}/\partial x_j)].\end{aligned} \tag{41}$$

If we apply Taylor's formula (as in Lemma 5), we have

$$(\partial t_i/\partial x_{j_1})(T^{-1}x + P_k T^{-1}x)(\partial t_i/\partial x_{j_1})(T^{-1}x) + \sum (\partial t_i/\partial x_{j_1}\partial x_l)(T^{-1}x + \theta_l P_k) f_l(Tx^{-1}).$$

Since $\sum (\partial t_i/\partial x_{j_1})(T^{-1}x)(\partial t^*{}_{j_1}/\partial x_y) = \partial x_i(TT^{-1}x)/\partial x_j = \delta^j{}_i$, (41) can be written as

$$\partial f_i^{k+1}/\partial x_j = \sum_{j_1, m_1} A_{ij_1}(\partial f^k{}_{j_1}/\partial x_{m_1}(T^{-1}x) B_{m_1} + P(i,j), \tag{42}$$

where

$$A_{ij} = (\partial n_i/\partial x_j)(T^{-1}x + P_k T^{-1}x), \tag{43}$$

$$B_{ij} = (\partial t^*{}_i/\partial x_j)(x), \tag{44}$$

and $P(i,j)$ is a polynomial in $\partial n_{j_1}/\partial x_{j_2}$, $\partial^2 n_{j_1}/\partial x_{j_2}\partial x_{j_3}$, $\partial t_{j_1}/\partial x_{j_3}$, $\partial g_i(T^{-1}x)/\partial x_{j_1}$, $f_i(T^{-1}x)$, whose form is independent of k and such that every monomial occurring in $P(i,j)$ contains at least one factor $\partial g_l/\partial x_{j_1}(T^{-1}x)$ or $f_l(T^{-1}x)$.

Similarly, by differentiating (41) the right number of times and by applying Taylor's formula to the appropriate terms, we have

$$\begin{aligned}&(-\partial^p f_i^{k+1}/\partial x_{l_1} \cdots \partial x_{l_p})(x) \\ &= \sum_{j, m_1, \cdots, m_p} A_{ij}(\partial^p f_j/\partial x_{m_1} \cdots \partial x_{m_p})(T^{-1}x) B_{m_1 l_1} \cdots B_{m_p l_p} \\ &\qquad + P(i, l_1, \cdots, l_p)(x),\end{aligned} \tag{45}$$

where the matrices A and B are given by (43) and (44), and $P(i, l_1, \cdots, l_p)$ is a polynomial in the partial derivatives of n and g of height at most p evaluated at various points in the sphere of radius $\| P_n \circ T^{-1}x \|$ about the point $T^{-1}x$, in the partial derivatives of height at most p of the $t^*{}_j$ evaluated

at x, in the partial derivatives of *height at most* $p-1$ of the $f^k{}_i$ evaluated at the point $T^{-1}x$.

We now prove Lemma 8 by induction on the height of the partial derivative.

Induction Hypothesis. For $m < l$, the partial derivatives $\partial^m f_i/\partial x_{l_1}\cdots\partial x_{l_m}$ are continuous in B_r, and for every q, there exists a constant A_q such that

$$(46)\qquad |(\partial^m f_i/\partial x_{l_1}\cdots\partial x_{l_m})(x)| < A_q \| x \|^q, \text{ for all } (i, l_1,\cdots, l_m).$$

We have proved this for $l=1$; we now assume it for $l=p-1$ and will now prove it for $l=p$.

Now since the g_i (and all its derivatives) vanish at the origin with infinite order, and the various partial derivatives of the t_i and n_i occurring in $P(i, l_1,\cdots, l_p)$ are bounded, for any q (using (46)), we can find a constant $A^*{}_q$ such that

$$(47)\qquad | P_i(i, l_1,\cdots, l_p)(x)| < A^*{}_q \| x \|^q.$$

Now we regard $(\partial^p f^k{}_i/\partial x_{l_1}\cdots\partial x_{l_p})(x)$ and $P(i, l_1,\cdots, l_p)(x)$ as the $(i, l_1,\cdots, l_p)$-th rectangular coordinate of vectors $\boldsymbol{f}_p{}^k$ and $\boldsymbol{P}(x)$ in a Euclidean space of m^{p+1} dimensions with the (Euclidean) norm $|||\cdot|||$. Then (45) can be written as

$$(48)\qquad \boldsymbol{f}_p{}^{k+1}(x) = \boldsymbol{H}(x)\cdot \boldsymbol{f}_p{}^k(T^{-1}x) + \boldsymbol{P}(x),$$

where $\boldsymbol{H}(x)$ is the linear transformation occurring in (45); it is the tensor product of A and p-times B. Thus, for a point x in $W_{k,r}$,

$$(49)\qquad \begin{aligned} \boldsymbol{f}_p{}^k(x) = \boldsymbol{P}(x) + \boldsymbol{H}(x)\boldsymbol{P}(T^{-1}x) + \boldsymbol{H}(x)\boldsymbol{H}(T^{-1}x)\boldsymbol{P}(T^{-2}x) \\ +\cdots+\boldsymbol{H}(x)\cdots\boldsymbol{H}(T^{-k}x)\boldsymbol{f}_p{}^0(x). \end{aligned}$$

In view of the construction of D in $W_{0,r}$ and (47), for any q, there is a constant $A^{**}{}_q$ such that

$$(50)\qquad |||\boldsymbol{f}_p{}^0(x)||| < A^{**}{}_q \| x \| \text{ for } x \in W_{0,r}$$

and

$$(51)\qquad |||\boldsymbol{P}(x)||| < A^{**}{}_q \| x \| \text{ for } x \in B_r.$$

Now let x^0 be a point of I_+ different from the origin. We wish to show that given any $\epsilon > 0$, there exists a $\delta > 0$ such that for any two points $x^1 \notin I_+$ and $x^2 \notin I_+$, in the sphere of radius δ and about x_0, we have

$$(52)\qquad |(\partial^p f_i/\partial x_{l_1}\cdots\partial x_{l_p})(x^1) - (\partial^p f_i/\partial x_{l_1}\cdots\partial x_{l_p})(x^2)| < \epsilon \quad \text{for all } (i, l_1,\cdots, l_p).$$

We can view $\partial^p f/\partial x_{l_1}\cdots\partial x_{l_p}$ as the components of the vector f_p as before and replace (52) by

$$(53)\qquad |||f_p(x^1)-f_p(x^2)|||<\epsilon.$$

Now the matrix $H(x)$ is uniformly bounded in norm since its entries are just polynomials in $\partial n_i/\partial x_j$ and $\partial t^*_i/\partial x_j$ evaluated at various points in B_r. Thus there is a constant M such that the norm of $H(x)$ is $\leqq M$. Now choose q so large that

$$(54)\qquad \kappa^q M=\alpha<1.$$

Applying the same method as was used to prove (37) to (49), we can find a constant K such that

$$
\begin{aligned}
(55)\quad |||f_p^k(x^1)-f_p^k(x^2)||| &\leqq |||\boldsymbol{P}(x^1)-\boldsymbol{P}(x^2)|||\\
&+|||\boldsymbol{H}(x^1)\boldsymbol{P}(T^{-1}x^1)-\boldsymbol{H}(x^2)\boldsymbol{P}(T^{-1}x^2)|||\\
&+\cdots+|||\boldsymbol{H}(x^1)\boldsymbol{H}(T^{-1}x^1)\cdots\boldsymbol{H}(T^{-m}x^1)\boldsymbol{P}(T^{m-1}x^1)\\
&\qquad-\boldsymbol{H}(x^2)\cdots\boldsymbol{H}(T^{-n}x^2)\boldsymbol{P}(T^{m-1}x^2)|||\\
&+K\alpha^m
\end{aligned}
$$

for all large k and all $m<k$. First choose m so large that

$$(56)\qquad K\alpha^m<\tfrac{1}{2}\epsilon.$$

Next choose δ_1 so small that if a point $x\notin I_+$ is in the ball of radius δ_1, then $x\in W_{k,r}$ with $k>m$. We now want to make each of the first m terms of the right hand side of (55) less than $\epsilon/2m$. This can be done as follows: By choosing δ sufficiently small, we can arrange that if x^1 is in the ball of the radius δ about x_0, then $T^{-1}x,\cdots,T^m x$ is in the ball of radius δ_2 about $T^{-1}x_0,\cdots,T^{-m}x_0$ respectively. Now for $y\to I_+$, $F(y)\to 0$ so that for any δ_3, we can choose δ_2 so small that all the derivatives of n_i occurring in the $P(i,l_1,\cdots,l_p)T^{-j}x$ $(j=0,\cdots,m)$ are evaluated at points in the ball of radius δ_3 about $T^j x$. Then by the continuity of the partial derivatives of the n_i, t^*_i, g_i, and the partial derivatives of the f_i of height $<p$, we can choose δ_3 so small that each of the first m terms is less than $\epsilon/2m$.

Now an elementary theorem in the theory of real variables (a simple consequence of Taylor's formula) asserts the following: if $u(x_1,\cdots,x_n)$ is a function defined and continuous in the neighborhood of a point x_0 lying on a plane I_+: $x_{k+1}=\cdots=x_n=0$, such that $\partial u/\partial x_i\leqq k$ exists and is continuous for all i everywhere in the enighborhood of the hyperplane and tends to a limit as $x\to x_0$, then $(\partial u/\partial x_i)(x_0)$ exists and is $\lim_{x\to x_0}(\partial u/\partial x_i)(x)$. Using this

theorem, applied to the partial derivatives of order $p-1$ of f at I_- ($f=0$ on I_+), we have established that f has continuous derivatives of order p at all points except the origin. But applying the previous argument, we can conclude that for any m, there exists a constant B_m such that

$$|(\partial^p f_i/\partial x_{l_1}\cdots\partial x_{l_m})(x)| < B_m |x|^m. \tag{57}$$

Thus the derivatives exist and are continuous (and vanish) at the origin too. We have thus proved

THEOREM 3. *Let $T\in \boldsymbol{G}^n$ and $N\in \boldsymbol{G}^n$ be such that $T-N$ vanishes at the origin with infinite order. Then there exists a $D\in \boldsymbol{G}^n$ such that $DT=ND$ and $D-E$ vanishes at the origin with infinite order. If the invariant surfaces of both N and T are I_+ and I_- and N coincides with T on these surfaces, then D can be chosen to be the identity in a one sided neighborhood of every point of the cone C other than the origin.*

Remark. Theorem 3 implies Theorems 1 and 3 of [14] by the trivial formal considerations of § 4 and of [10] and Lemma 5 of [14].

6. In this section we show that any element T of $\boldsymbol{V}^n$ satisfying (**) lies on a one parameter group. By Theorem 3 and Lemma 4, $T=DND^{-1}$, where $N\in \boldsymbol{C}^n$, $D\in \boldsymbol{G}^n$. Now any element of $\boldsymbol{C}^n$ can clearly be embedded in a one-parameter group of volume preserving transformations. Therefore, there exists a one parameter family T^*_t such that $T^*_1=T$ and such that the Jacobian of T^*_t tends to one with infinite order at the origin. If $v=(v_1,\cdots,v_n)$ denotes the vector field corresponding to this flow, then $\operatorname{div} v=\sum \partial v_i/\partial x_i$ vanishes at the origin with infinite order. We now show that we can modify T^*_t so as to become volume preserving. That is we shall prove

THEOREM 4. *Every $T\in \boldsymbol{V}^n$ satisfing (**) lies on a one parameter group $T_s\in \boldsymbol{V}^n$.*

If we consider the vector field v, the equation for a multiplier u so that the field uv be divergence free is

$$\sum \partial(uv_i)/\partial x_i=\sum (\partial u/\partial x_i)v_i+u(\operatorname{div} v)=0 \tag{58}$$

If we write $u(x_1,\cdots,x_n)$ as $u(x_1(t),\cdots,x_n(t))$, then (58) becomes the ordinary differential equation

$$du/dt=-u(\operatorname{div} v) \tag{59}$$

along each orbit. The general solution of (59) is

$$u(t) = K \exp\left(-\int_0^t \operatorname{div} v(r)\, dr\right).$$

We wish to choose K so that

$$\int_t^{1+t} u(r)\, dr = 1. \tag{60}$$

This can be done if and only if

$$\int_t^{1+t} \operatorname{div} v(r)\, dr = 0. \tag{61}$$

However (61) follows from the fact that T is volume preserving. We thus choose u by (59) and (60) for any point x not on I_+ or I_-. This can be done since $T_t(C)$ sweeps out a whole neighborhood of the origin except for these surfaces. If we set $u = 1$ on $I_+ \cup I_-$, it is easy to see that u is C^∞. Then the one parameter group T_s generated by the vector field uv satisfies the conclusions of the theorem.

Remark. In view of the choice of D, uv agrees with the vector field generating the one parameter group containing N in a one sided neighborhood of every point of C different from the origin.

7. In this section we conclude the proof of Theorem 1.

The cone C is a cross-section to the flow T_s given by Theorem 4 and also to the flow N_s on which N lies. Now, as in § 5, $T_s(C)$, for $\infty < s < +\infty$, sweeps out a whole neighborhood of the origin except for I_+ and I_-. Similarly, $N_s(C)$ sweeps out a whole neighborhood except for I_+ and I_-. Thus, if $y_1, \cdots, y_{n-1}$ denote coordinates on C, we can write, for $x = (x_1, \cdots, x_n) \notin I_+ \cup I_-$,

$$x_i = x_{i_T}(y_1, \cdots, y_{n-1}, t). \tag{62}$$

Now

$$\begin{aligned}(\partial/\partial t)\,(\partial(x_{1_T}, \cdots, x_{n_T}/\partial(y_1, \cdots, y_{n-1}, t)) \\ = (\partial(x_{1_T}, \cdots, x_{n_T}/\partial(y_1, \cdots, y_{n-1}, t)) \qquad (\operatorname{div} uv) = 0.\end{aligned} \tag{63}$$

Thus we can write

$$\partial(x_{1_T}, \cdots, x_{n_T})/\partial(y_1, \cdots, y_{n-1}, t) = A(y_1, \cdots, y_{n-1}). \tag{64}$$

If we do the same for N, we have, for $x \notin I_+ \cup I_-$,

$$x_i = x_{i_N}(y_1, \cdots, y_{n-1}, t). \tag{65}$$

In view of the last remark of § 6, we have

$$(66) \qquad \partial(x_{1_N}, \cdots, x_{n_N})/\partial(y_1, \cdots, y_{n-1}, t) = A(y_1, \cdots, y_{n-1}).$$

Thus if we compose the inverse of (62) with (65), we obtain a volume preserving transformation R. We can describe R as follows: if $x = T_s y$ $(y \in C)$, then $Rx = N_s y$. It is clear that R is now defined on an entire neighborhood of the origin and satisfies $RT = NR$. Furthermore, since T and N differ by terms vanishing at the origin with infinite order, R tends to the identity with infinite order at the origin. All that remains to be proved is that R is C^∞ along I_+ and I_-. However, this follows as in § 5.

8. We now consider the group $\boldsymbol{U}^n$ of those local C^∞ mappings which preserve volume up to a constant factor; that is, a map belongs to $\boldsymbol{U}^n$ if and only if its Jacobian determinant is constant. It is clear that the collection of such local maps form a group whose image under the projection onto linear terms is the general linear group $GL(n)$. It follows, as in Section 1, that the subgroups of transformations of the form (i) are maximal commutative subgroups of $\boldsymbol{U}^n$. We now wish to prove

THEOREM 5. *Let $T \in \boldsymbol{U}^n$ have linear part, L, of the form* (i) *and satisfy* (*). *Then there exists an $R \in \boldsymbol{U}^n$ (indeed $\in \boldsymbol{V}^n$) such that*

$$(67) \qquad RTR^{-1} = L.$$

We know, by Theorem 1 of [13], that there exists on $R \in \boldsymbol{G}^n$ satisfying (67). The problem is to construct an $R \in \boldsymbol{U}^n$ satisfying (67). We proceed, as usual, in two steps, first proving the corresponding formal theorem.

THEOREM 6. *Let $\mathfrak{U}^n$ be the group of formal power series transformations with constant Jacobian. Then if $T \in \mathfrak{U}^n$ has its linear part L of the form* (i) *and satisfies* (*), *there exists an $R\,\mathfrak{U}^n$ such that* (67) *holds.*

The proof of Lemma 1 of [9] shows that if we require the linear part of R to be the identity, equation (67) has a unique solution. What we must show is that this solution is indeed volume preserving; i. e., using the notation of (15), that $\Delta(x_1, \cdots, x_n) = \Delta(x) = 1$. Now in view of (67) and the fact that $T \in \mathfrak{U}^n$, the formal power series Δ satisfies

$$(68) \qquad \Delta(Lx) = \Delta(x).$$

Comparing coefficients, and noticing that (*) implies that $\lambda_1^{m_1} \cdots \lambda_n^{m_n} \neq 1$ for any positive integers m_i, yields $\Delta \equiv 1$, proving the theorem.

Lemma 3 carries over immediately to the present situation, as do all of the considerations of the previous sections up to the remarks preceding

Theorem 4. That is, after a preliminary change of coordinates belonging to U^n, we can assume that $T-L$ vanishes at the origin with infinite order, and that T lies on a one-parameter group of transformations T_t (not necessarily lying in U^n). We now prove the analogue of Theorem 4.

THEOREM 7. *Any $T \in U^n$ lies on a one parameter group T_s in U^n.*

In case $J(T)=1$, this follows from Theorem 4. Thus we may assume that $J(T)=a\neq 1$. If v denotes the vector field generating the flow $T^*{}_t$, then the equation for a multiplier u so that the vector field uv generates a one parameter subgroup of U^n is

$$\operatorname{div} uv = \alpha = \log a. \tag{69}$$

As in Section 6, this is equivalent to the ordinary differential equation

$$du/dt + u \operatorname{div} v = \alpha \tag{70}$$

along each orbit. The general solution of this equation is

$$u = 1/F(t)\left[\alpha \int_0^t F(s)\,ds + C\right], \tag{71}$$

where $F(t) = \exp \int_0^t \operatorname{div} v(s)\,ds$. We wish to choose C so that (69) holds. Now $\int_1^{1+x} \operatorname{div} v\,dt = \alpha$ since $T \in U^n$. Therefore, if we divide (70) by u and integrate from x to $1+x$, we find that (69) can be satisfied if we can choose C in (70) so that

$$\log u(1+x) - \log u(x) = 0; \tag{72}$$

since $\log F(1+x) - \log F(x) = \alpha$, we must choose C so that

$$\log\left[\alpha \int_0^{x+1} F(s)\,ds + C\right] - \log\left[\alpha \int_0^x F(s)\,ds + C\right] = \alpha. \tag{73}$$

Differentiating (72), we obtain

$$\left(\alpha \int_0^{x+1} F(x)\,ds + C\right)/F(x+1) = \left(\alpha \int_0^x F(s)\,ds + C\right)/F(x),$$

or

$$\alpha \int_0^{x+1} F(s)\,ds + C = \alpha \int_0^x F(s)\,ds + C). \tag{74}$$

Differentiating once more, we obtain an identity. We must thus choose $C = (a-1)^{-1}\alpha \int_0^1 F(s)\,ds$. Thus, if we take this value for C, we find that

$$r_i = x_i + \sum r^i_{j_1\cdots j_n, r_1\cdots r_n} x_1^{j_1}\cdots x_n^{j_n} y_1^{j_1}\cdots y_n^{j_n}$$

(83) and

$$s_i = y_i + \sum s^i_{j_1\cdots j_n, r_1\cdots r_n} x_1^{j_1}\cdots x_n^{j_n} y_1^{j_1}\cdots y_n^{j_n},$$

and set $N = (x_2 f_1(\omega_1,\cdots,\omega_n),\cdots, y_1 g_1(\omega_1,\cdots,\omega_n),\cdots)$, where

$$f_i = \lambda_i x_i + x_i \sum f^i_{j_1\cdots j_n}\omega_1^{j_1}\cdots\omega_n^{j_n}$$

(84) and

$$g_i = \lambda_i^{-1} y_i + y_i \sum g^i_{j_1\cdots j_n}\omega_1^{j_1}\cdots\omega_n^{j_n}.$$

If we substitute (83) and (84) into the equation $RTR^{-1} = N$, we obtain

$$\begin{aligned} r^i_{j_1\cdots j_n, k_1\cdots k_n}\lambda_1^{j_1-k_1}\cdots\lambda_n^{j_n-k_n} + \delta_{j_1}^{k_1+\delta_i^1}\cdots\delta_{j_n}^{k_n+\delta_i^n} f^i_{j_1\cdots j_n} \\ = \lambda_i r^i_{j_1\cdots j_n, k_1\cdots k_n} + \cdots, \end{aligned} \tag{85}$$

where the $\cdots$ indicate terms of lower height, and a similar set of equations for the s's. Thus if $j_p \neq k_p + \delta_i^p$ for some p, then condition (***) implies that $r^i_{j_1\cdots j_n, k_1\cdots k_n}$ is determined by the terms of lower height. If $j_p = k_p + \delta_i^p$ holds for all p, then $r^i_{j_1\cdots j_n, k_1\cdots k_n}$ is undetermined, whereas the corresponding term in f is. We wish to choose the undetermined terms in R so that $R \in \mathfrak{H}^n$ as we did in Section 2 for $\mathfrak{B}^n$. We choose the undetermined in R so that

$$\begin{aligned} &\sum_{i=1}^n [r_i, s_i]_{x_j x_k} \text{ contains no term of the form } y_j y_k \omega_1^{l_1}\cdots\omega_n^{l_n}, \\ &\sum_{i=1}^n [r_i, s_i]_{x_j y_k} - \delta_j^k \text{ contains no term of the form } y_j x_k \omega_1^{l_1}\cdots\omega_n^{l_n}, \\ &\sum_{i=1}^n [r_i, s_i]_{y_j y_k} \text{ contains no term of the form } x_j x_k \omega_1^{l_1}\cdots\omega_n^{l_n}. \end{aligned} \tag{86}$$

We will see later that such choice is possible. We first show that if (86) is satisfied, then R (and hence N) is Hamiltonian. We first remark that if $(x, y) \to (x^*, y^*)$ and $(x^*, y^*) \to (x^{**}, y^{**})$ are two smooth transformations, then

$$\begin{aligned} [x^{**}_i, y^{**}_i]_{x_j x_k} = &\sum_{l<m} [x^{**}_i, y^{**}_i]_{x^*_l x^*_m}(x^*_l, y^*_l)[x^*_l, x^*_m]_{x_j x_k} \\ &+ \sum_{l,m} [x^{**}_i, y^{**}_i]_{x^*_l y^*_m}(x^*, y^*)[x^*, y^*]_{x_j x_k} \\ &+ \sum_{l<m} [x^{**}, y^{**}]_{y^*_l y^*_m}(x^*, y^*)[x^*, y^*]_{x_j x_k}, \end{aligned} \tag{87}$$

with similar formulae for $[x^{**}_i, y^{**}_i]_{x_j y_k}$ and $[x^{**}_i, y^{**}_i]_{y_j y_k}$.

In particular, if the transformation $(x^*, y^*) \to (x^{**}, y^{**})$ is Hamiltonian, then

$$\sum_i [x^{**}_i, y^{**}_i]_{x_j x_k} = \sum_i [x^*_i, y^*_i]_{x_j x_k}. \tag{88}$$

If we now apply (87) to RN and (88) to TR, we obtain

$$\begin{aligned} \sum_i \sum_{l<m} [s_i, r_i]_{y_l y_m}(xf, yg)\,[x_l f_l, x_m f_m]_{x_j x_k} \\ + \sum_i \sum_{l,m} [s_i, r_i]_{x_l y_m}(xf, yg)\,[x_l f_l, y_m g_m]_{x_j x_k} \\ + \sum_i \sum_{l<m} [s_i, r_i]_{y_l y_m}(xf, yg)\,[y_l g_l, y_m g_m]_{x_j x_k} \\ = \sum_i [r_i, s_i]_{x_j x_k}. \end{aligned} \tag{89}$$

Let us prove

$$\sum_i [r_i, s_i]_{x_j x_k} = 0, \tag{90}$$

for all s, r. It is clear that the linear terms on the left hand side of (90) do vanish. We shall assume that all terms of height smaller than N vanish. If we compare the coefficients of $x_1^{l_1} \cdots x_n^{l_n} y_1^{m_1} \cdots y_n^{m_n}$ in (89), we obtain

$$\begin{aligned} &(\sum_i [r_i, s_i]_{x_j x_k})_{l_1 \cdots l_n, m_1 \cdots m_n} \\ &\quad = \lambda_j^{-1} \lambda_k^{-1} \lambda_1^{l_1 - m_1} \cdots \lambda_n^{l_n - m_n} (\sum_i [r_i, s_i]_{x_j x_k})_{l_1 \cdots l_n, m_1 \cdots m_n} + \cdots, \end{aligned} \tag{91}$$

where the $\cdots$ are terms of lower height. Now by Lemma 9, the second term on the right of (91) will vanish unless $l_p = m_p + \delta_j^p + \delta_k^p$. If $l_p \neq m_p + \delta_j^p + \delta_k^p$ for some p, then (91) and (***) imply that

$$(\sum_i [r_i, s_i]_{x_j x_k})_{l_1 \cdots l_n, m_1 \cdots m_n} = 0. \tag{92}$$

On the other hand, if $l_p = m_p + \delta_j^p + \delta_k^p$ for all p, then the choice (86) implies (91). A similar argument, establishes (77) and (78) for $x^*_i = r_i$, $y^*_i = s_i$.

All that remains to be proved is that we can arrange for (85) to be statisfied. In order to show this, we first observe that in order for a map $(x, y) \to (x^*, y^*)$ to be Hamiltonian and have the identity as Jacobian matrix at the origin, it is necessary and sufficient that there exist a function $H(x, y)$ such that

$$x^*_i = \partial H(x, y^*)/\partial y^*_i \text{ and } y_i = \partial H(x, y^*)/\partial x_i. \tag{93}$$

In fact, (75) is equivalent to

$$\sum x^*_i dy^*_i + \sum y_i dx_i = dH. \tag{94}$$

If we introduce x_i and y^*_i as coordinates, then (93) follows from (94). If

now $(x,y)\rightarrow(x^*,y^*)$ is a transformation satisfying (76), (77), and (78) up through terms of order n, then

$$\sum_i x^*_i dy^*_i+\sum_i y_i dx_i=dH+\Omega, \tag{95}$$

where Ω is a linear differential form all of whose coefficients vanish at the origin with order $n+1$. That is, (x^*,y^*) satisfies (92) up through terms of order n. If we replace (x^*,y^*) by exact solutions we shall obtain a Hamiltonian map. Thus, if a mapping $(x,y)\rightarrow(x^*,y^*)$ satisfies (76), (77), and (78) up to order n, we can arrange that these equations hold identically by *changing the terms of degree* $>n$ only. Thus if we are given the expansion of R up to order n, we can choose the terms of degree $n+1$ so that R be Hamiltonian up to degree n. However, the only terms of degree $n+1$ in R which can contribute anything to the terms of degree n on the right hand side of (85) are precisely those which are at our disposal. Thus (85) can be satisfied, completing the proof of Theorem 8.

An argument similar to the one given in the preceding paragraph yields the analogue to the present situation of Lemma 3. In trying to apply the techniques of § 5 to the Hamiltonian group, we are faced with a fundamental difficulty. The argument there depends essentially on the fact that no eigenvalue is of absolute value one. This is not, however, implied by (***); we must therefore make the additional assumption. We have thus progressed to the situation analogous to that just before the proof of Theorem 4. The same techniques used to prove Theorem 4 do not apply to the present situation. This is clear, since given a vector field, one can not, in general, find a multiplier which will make it Hamiltonian. However, one can replace the device used in proving Theorem 5 via Theorem 4 by a more pedestrian 'filling in' process applied directly to prove Theorem 5, the details of which we will not bother with here. Modulo these considerations, we have thus proved

THEOREM 9. *Let $T\in \boldsymbol{H}^n$ satisfy* (***) *and have no eigenvalue of absolute one. Then there exists an $R\in\boldsymbol{H}^n$ such that RTR^{-1} is of the form* (80).

RIAS INC. AND THE UNIVERSITY OF CHICAGO.

REFERENCES.

[1] G. D. Birkhoff, "Surface transformations and their dynamical applications," *Collected Mathematical Papers*, vol. II, pp. 111-229.

[2] ———, "Nouvelles recherches sur les systemes dynamiques," *Collected Mathematical Papers*, vol. II, pp. 590-620.

[3] ———, *Dynamical Systems*, American Mathematical Society Colloquium Publications, vol. IX (1927), pp. 59-96.

[4] E. Cartan, "Sur la structure des groupes infinies de transformations," Oeuvres, Partie II, vol. 2, pp. 571-715.

[5] S. S. Chern, "Pseudo-groupes continus infinies," *Colloque de géométrie differentielles, Strassbourg* (1953), pp. 110-136.

[6] A. Finzi, "Sur le problème de la génération d'une courbe fermee par une transformation infinitésimale," *Annales de l'Ecole Normale Superieure*, vol. 67 (1950), pp. 243-305.

[7] M. Kuranishi, "On the abstract approach to the local theory of infinite continuous pseudogroups" (mimeographed), Chicago, 1957.

[8] P. Liberman, "Sur le probleme d'equivalence de certaine structures infinitesimales," *Annali di Matematica*, Ser. 4, vol. 36 (1954), pp. 27-120.

[9] H. Poincaré, Oeuvres, vol. 1.

[10] J. Moser, "The analytic invariants of an area preserving mapping near hyperbolic point," *Communications on Pure and Applied Mathematics*, vol. 19 (1956), pp. 673-692.

[11] C. L. Siegel, *Vorlesungen über Himmelsmechanik*, Springer Verlag, 1957.

[12] ———, "Vereinfachter Beweiss eines Satzes von J. Moser," *Communications on Pure and Applied Mathematics*, vol. 10 (1957), pp. 305-309.

[13] S. Sternberg, "Local contractions and a theorem of Poincaré," *American Journal of Mathematics*, vol. 79 (1957), pp. 809-823.

[14] ———, "The structure of local homeomorphisms, II," *American Journal of Mathematics*, vol. 80 (1958), pp. 623-632.

L'APPROXIMATION POLYNOMIALE PONDEREE SUR UN ESPACE LOCALEMENT COMPACT.*

par PAUL MALLIAVIN.

L'approximation polynomiale par Weierstrass de toute fonction continue sur $[0, 1]$ a des équivalents classiques pour des intervalles non compacts. Par exemple, l'approximation sur $[0, +\infty)$ par les polynômes de Laguerre multipliés par le poids e^{-x}, ou celle sur $(-\infty, +\infty)$ par les polynômes d'Hermite, le poids étant alors e^{-x^2}. On se propose d'étudier ce problème dans le cadre général dans lequel M. H. Stone [6] a démontré le théorème de Weierstrass.

Le procédé utilisé consistera à se ramener au même problème d'approximation avec une seule variable, problème déjà envisagé par S. Bernstein, S. Mandelbrojt [3], H. Pollard [5]. Ce procédé de réduction donnera en particulier une démonstration du théorème de Stone-Weierstrass n'utilisant pas la structure d'ordre sur l'espace des fonctions continues réelles ([1] et [6]) ce qui permettra d'étendre le résultat de Stone à des algèbres complexes, moyennant des conditions analogues à celles de Mergelyan [4].

1. Notations et énoncés. E étant un espace localement compact, on notera par $C(E)$ l'algèbre des fonctions continues à valeurs complexes définies sur E, par $C_0(E)$ la sous-algèbre des fonctions $f(x)$ tendant vers zéro lorsque x tend vers l'infini; $C_0(E)$ est une algèbre de Banach pour la norme usuelle

$$\| f \| = \max | f(x) |.$$

Si F désigne une partie de $C(E)$, on notera par $\mathfrak{A}_F$ la plus petite sous-algèbre contenant F ainsi que l'unité; tout élément de $\mathfrak{A}_F$ s'écrit comme un polynôme formé avec un nombre fini d'éléments de F.

Si $F \subset C_0(E)$, le problème d'approximation à partir des éléments de F se ramène au même problème sur un espace compact en compactifiant E par l'adjonction d'un point à l'infini. Ce cas a été envisagé par M. H. Stone dans [6].

* Received September 26, 1958; Revised October 19, 1958.

Si $F \not\subset C_0(E)$ alors pour pouvoir approcher des éléments de $C_0(E)$, il est nécessaire d'introduire une fonction $p(x) \in C_0(E)$ telle que $p\mathfrak{A}_F \subset C_0(E)$.

On dira que p est *un poids* (pour la famille F) si $p\mathfrak{A}_F \subset C_0(E)$ et si $p\mathfrak{A}_F$ est dense dans $C_0(E)$.

Deux conditions nécessaires évidentes pour que p puisse être un poids:

$p(x) \neq 0$ pour tout $x \in E$;

F est une famille séparante, c'est à dire que

$f(x) = f(x')$ pour tout $f \in F$ entraine $x = x'$.

Dans toute la suite nous supposerons ces conditions satisfaites.

Remarquons que si p et p_1 sont deux fonctions définies sur E telles que $p = 0(p_1)$, que $p_1\mathfrak{A}_F \subset C_0(E)$ et que p soit un poids, alors p_1 est un poids. Sinon on pourrait trouver une mesure $d\mu$ orthogonale à $p_1\mathfrak{A}_F$, la mesure $(p/p_1)\,d\mu = d\rho$ serait orthogonale à $p\mathfrak{A}_F$ et satisferait à $\int |d\rho| = 0(\int |d\mu|) < \infty$. p étant un poids, $d\rho = 0$ d'où $d\mu = 0$.

En particulier si E est compact $p = 0(1)$, et $1 = 0(p)$, l'approximation pondérée est équivalente dans ce cas à l'approximation ordinaire.

Enonçons le résultat le plus simple qui permet de reconnaître un poids:

1.1. *Si pour tout $f \in F$, p est à valeurs réelles et*

$$\sum \| pf^n \|^{-1/n} = \infty,$$

alors p est un poids.

Le procédé de démonstration consistera à se ramener au problème à 1 variable suivant. Si e désigne une partie fermée du corps complexe, M_n une suite de nombres positifs, *on dit que la proposition $R(e, M_n)$ est vérifiée* si toute mesure $d\mu$ de support e vérifiant

$$\int z^n \, d\mu = 0 \text{ pour tout } n \geqq 0, \qquad \int |z|^n \, |d\mu| \leqq M_n$$

est identiquement nulle.

On dira que $R^*(e, M_n)$ vaut si quel que soit l'entier $s \geqq 0$, $R(e, (M_{2^s n})^{2^{-s}})$ vaut.

On a alors l'énoncé de réduction à 1 variable suivant:

1.2. *Si $R^*(\overline{f(E)}, \| pf^n \|)$ vaut pour tout $f \in F$, alors p est un poids.*

En appliquant au cas compact et en utilisant le théorème de Mergelyan, à savoir: si e une partie compacte non dense du plan complexe, ne séparant pas le plan, alors les polynômes en z sont denses dans l'espace des fonctions

continues sur e, on obtient l'extension suivante du théorème de Mergelyan à un espace compact:

1.3. *Si E est compact, et si pour tout $f \in F$, $f(E)$ est un ensemble non dense, ne séparant pas le plan complexe, alors $\mathcal{A}_F$ est dense dans $C(E)$.*

On peut désirer avoir l'equivalent de 1.3 dans le cas non compact, on obtient l'énoncé suivant contenant 1.1.

1.4. *Supposons que pour tout $f \in F$, $f(E)$ soit un ensemble de mesure superficielle nulle, le complémentaire de $\overline{f(E)}$ se composant de domaines $\Omega_1, \cdots, \Omega_k$, chaque domaine Ω contenant à son intérieur un angle d'ouverture ϕ, et que*

$$\sum \| pf^n \|^{-\pi/\phi n} = \infty,$$

alors p est un poids.

Nous allons commencer par démontrer 1.2.

2. Si la conclusion de 1.2, n'était pas vérifiée, on pourrait trouver une mesure dv portée par E telle que pour tout $f \in F$ et tout n

$$\int pf^n \, dv = 0, \qquad \int | dv | < \infty.$$

Nous allons étudier la projection de cette mesure sur des ensembles de dimension finie.

Si F_1 désigne une partie de F, $\bar{C}$ la sphère de Riemann, c'est-à-dire le plan complexe auquel on a adjoint un point à l'infini, $\bar{C}^{F_1}$ l'espace compact produit de F_1 exemplaires de $\bar{C}$, on a une application continue $h_{F_1}: E \to \bar{C}^{F_1}$ qui à tout $x \in E$ associe $\{f(x)\}_{f \in F_1}$. À la mesure $d\mu$ définie sur E, on associe son image par h_{F_1}, $d\mu_{F_1} = h_{F_1}(d\mu)$, définie par l'égalité

$$\int g(y) \, d\mu_{F_1}(y) = \int g(h_{F_1}(x)) \, d\mu(x)$$

On a alors le lemme:

2.1. *Si pour toute partie finie ϵ de F $d\mu_\epsilon = 0$, alors $d\mu = 0$.*

Démonstration. Soit K une partie compacte de E, g une fonction réelle, continue sur E, de support contenu dans K. La famille F étant séparante, l'application $h_F: E \to \bar{C}^F$ est biunivoque, sa restriction à K est un homéomorphisme et $g \circ h_F^{-1}$ est une fonction continue sur le compact $h_F(K)$. Réalisant un recouvrement de $h_F(K)$ par des ouverts de la forme

$$0 = \{y\,; y \in h_F(K) \text{ et } | f_i(h_F^{-1}(y)) - a_i | < b_i, i = 1, \cdots, n\}$$

on peut trouver un recouvrement fini de tels ouverts tel que si y et y' appartiennent au même ouvert, on ait

$$|g(h_F^{-1}(y)) - g(h_F^{-1}(y'))| < \eta.$$

Notons par ϵ la partie finie de F constituée par toutes les fonctions f servant à définir les ouverts de ce recouvrement.

On aura en particulier:

$$|g(x) - g(x')| < \eta \text{ pour tout } x \text{ et } x' \text{ vérifiant } h_\epsilon(x) = h_\epsilon(x')$$

Introduisons maintenant la fonction

$$k(x) = \max_{x'} g(x') \text{ où } x' \text{ est assujetti à la condition } h_\epsilon(x') = h_\epsilon(x).$$

On sait que (cf. Bourbaki [2], Chap. V, p. 32) $k(x)$ est une fonction semi-continue supérieurement vérifiant $0 \leqq k(x) - g(x) < \eta$; d'autre part, il existe une fonction l définie sur $h_\epsilon(K)$, semi-continue supérieurement, telle que

$$k(x) = l(h_\epsilon(x)).$$

On aura alors

$$\left| \int g(x)\, d\mu(x) - \int k(x)\, d\mu(x) \right| \leqq \eta \,\|\mu\|,$$

$$\int k(x)\, d\mu(x) = \int l(y)\, d\mu_\epsilon(y) = 0.$$

η étant arbitraire, on obtient $\int g(x)\, d\mu(x) = 0$, d'où $d\mu = 0$ ce qu'il fallait démontrer.

Le lemme précédent ramène le problème d'approximation sur un espace localement compact à l'approximation sur les parties de l'espace complexe à m dimensions C^m. Nous allons ramener ce problème au problème à une variable $R^*(e, M_n)$.

2.2. *Soit E une partie de C^m, e_k sa projection sur le $k^{\text{ème}}$ plan complexe de coordonnées, soit $d\mu$ une mesure de support E; posons*

$$\|g\|_\mu = \int |g(z_1, \cdots, z_m)|\, |d\mu(z_1, \cdots, z_m)|.$$

Supposons que

$$R^*(\bar{e}_k, \|z_k{}^n\|_\mu)$$

soit vérifié, $1 \leqq k \leqq m$, et que $d\mu$ soit orthogonale à tous les polynômes en $z_1, z_2, \cdots, z_m$; alors $d\mu = 0$.

Démonstration. Si $m = 1$, faisant $s = 0$ dans la définition de R^* donnée en 1, on obtient que $R(e_1, \|z_1{}^n\|_\mu)$ est vérifié, d'où par définition même que $d\mu = 0$. Nous allons établir une récurrence sur la dimension m.

Soit l la projection $C^m \to C^{m-1}$ $(z_1, z_2, \cdots, z_m) \to (z_2, \cdots, z_m)$,

t la projection $C^m \to C$ $(z_1, z_2, \cdots, z_m) \to z_1$,

q étant un entier fixé, projetons par l la mesure $z_1{}^q\, d\mu$.

$l(z_1{}^q\, d\mu) = d\rho$ est porté par C^{m-1}, vérifie

$$\int P(z_2, \cdots, z_m)\, d\rho = 0$$

et d'autre part,

$$\| z_k{}^n \|_\rho < \int | z_k{}^n | \, | z_1{}^q | \, | d\mu |, \qquad k = 2, \cdots, m.$$

Appliquons l'inégalité de Schwarz, on obtient

$$\| z_k{}^n \|_\rho \leqq \| z_k{}^{2n} \|_\mu{}^{\frac{1}{2}} \| z_1{}^{2q} \|_\mu{}^{\frac{1}{2}}.$$

De cette inégalité il résulte que les propositions $R(\bar{e}_k, \| z_k{}^{2n} \|_\mu{}^{\frac{1}{2}})$, $k = 1, 2, \cdots, m$, entrainent les propositions $R(\bar{e}_k, \| z_k{}^n \|_\rho)$, $k = 2, \cdots, m$, ou en passant à R^*, on obtient que $R^*(\bar{e}_k, \| z_k{}^n \|_\rho)$ est vérifié. La conclusion de 2.3. était supposée vraie pour $m - 1$, $d\rho = 0$, ce qui peut s'écrire

$$\int k(z_2, z_3, \cdots, z_m) z_1{}^q\, d\mu = 0$$

quelle que soit la fonction continue k à support compact. Projetons maintenant par t la mesure $k\, d\mu$ sur C, soit $d\sigma = t(k\, d\mu)$. On a

$$\| z_1{}^n \|_\sigma \leqq \int | z_1 |^n \, | k | \, | d\mu | < \| k \| \, \| z_1{}^n \|_\mu$$

d'où en appliquant $R^*(\bar{e}_1, \| z_1{}^n \|_\mu)$ on conclut que $d\sigma = 0$, ce qui s'écrit

$$\int k_1(z_1) k(z_2, \cdots, z_n)\, d\mu = 0$$

quelle que soit la fonction continue à support compact k_1. Les produits $k_1 k$ et leurs combinaisons linéaires étant denses dans $C_0(E)$, on obtient $d\mu = 0$.

2.3. Preuve de 1.2.

Soit dv une mesure orthogonale à $p\mathfrak{a}_F$; posons $d\mu = p\, dv$, et si ϵ est une partie finie de F, soit $d\mu_\epsilon$ la projection de $d\mu$ sur C^ϵ. Alors on a

$$\| z_i{}^n \|_{\mu_\epsilon} < \int | f_i{}^n | \, | p\, dv | < \| p f_i{}^n \| \int | dv |.$$

Appliquons 2.2 à $d\mu_\epsilon$, on obtient $d\mu_\epsilon = 0$; 2.1 donne $d\mu = 0$, $p(x) \neq 0$ ceci entraine $dv = 0$. c. q. f. d.

3. Nous allons étudier dans un cas simple la proposition $R^*(e, M_n)$.

3.1. *Supposons que e soit mesure superficielle nulle et que chaque com-*

posante connexe du complémentaire de e contienne un angle 0 *d'ouverture* ϕ $(0 < \phi < 2\pi)$, *c'est à dire* $\{z; |\arg(z-z_0)-\alpha| \leqq \frac{1}{2}\phi\}$. *Alors si*

$$\sum M_n^{-\pi/\phi n} = \infty,$$

$$R(e, M_n) \text{ est vérifié.}$$

Démonstration. Soit $d\mu$ une mesure vérifiant les hypothèses de $R(e, M_n)$. Posons

$$F(z) = \int d\mu(\xi)/(z-\xi).$$

L'identité

$$1/(z-\xi) = \sum_{p<n} \xi^p/z^p + \xi^n/z^n(z-\xi)$$

donne

$$|F(z)| = |z^{-n} \int \xi^n d\mu(\xi)/(z-\xi)| \leqq \|\xi^n\|_\mu |z|^{-n} d_e^{-1}(z),$$

d_e désignant la distance de z à e. On peut en modifiant le sommet z_0 de angle O se ramener au cas où $d_e^{-1}(z) < 1$, $z \in O$. $F(z)$ sera alors une fonction holomorphe dans O vérifiant

$$|F(z)| < M_n/|z^n| \text{ pour tout } n \geqq 0,$$

d'où $F(z) = 0$, $z \in O$. (Cf. par exemple [3], p. 27.). Il en résulte que $F(z)$ sera nul sur la composante connexe contenant O, et ainsi $F(z) = 0$ dans le complémentaire de e, c'est à dire $F(z) = 0$ sauf peut-être sur un ensemble de mesure nulle.

Soit $d\lambda$ la mesure ayant une densité superficielle égale à i sur la couronne $r < |z-z_1| < R$. Alors

$$\int d\lambda(\xi)/(-z+\xi) = \psi(z)$$

vérifie $\psi(z) = \text{constante} \neq 0$ si $|z-z_1| < r$,

$$\psi(z) = 0 \qquad \text{si } |z-z_1| > R,$$

$$0 \leqq \psi(z) \leqq \psi(z_1).$$

Lorsque l'on fait varier z_1, r, R, les combinaisons linéaires des fonctions ψ sont donc denses dans l'espace des fonctions continues à support compact définies sur le plan complexe.

D'autre part, le théorème de Fubini permet d'écrire

$$\int \psi(z) d\mu(z) = -\int F(\xi) d\lambda(\xi).$$

F étant nul presque partout, cette dernière intégrale est nulle, d'où $d\mu = 0$.

Remarquons que ce résultat vaut encore si e est contenu sur l'axe réel positif. Il convient alors de prendre $\phi = 2\pi$, comme on le voit en effectuant la représentation conforme $z \to (-z)^{\frac{1}{2}}$.

3.2. Pour passer des relations R aux relations R^* on utilisera les remarques de convexité suivantes:

Soit M_n une suite telle que $\log M_n$ soit convexe, α une constante; alors les séries $\sum M_n^{-\alpha/n}$ et $\sum M_{2n}^{-\alpha/2n}$ sont équiconvergentes. En effet, la seconde série est extraite de la première et d'autre part la convexité implique que pour n assez grand

$$\log M_n < \tfrac{1}{2} \log M_{2n}$$

D'autre part si $\| f^n p \| = M_n$, alors $\log M_n$ est une suite convexe; en effet, si on pose $\psi_x(z) = | f(x) |^z . p(x)$, alors $\log \ | \psi_x(z) |$ est une fonction harmonique de z, par suite

$$\log \| \, | f |^z p \, \| = \sup_x \log | \psi_x(z) |$$

est une fonction sous-harmonique de z, ne dépendant que de $\operatorname{Re} z$, donc c'est une fonction convexe de $\operatorname{Re} z$.

Ces remarques étant faites, la divergence de la série 3.1 implique la relation $R^*(e, \| pf^n \|)$. L'application de 1.2 donne alors la démonstration de 1.4.

Par exemple, si on applique 1.4 au poids e^{-z} on obtient que l'approximation par les polynômes de Laguerre multipliés par e^{-z} est possible sur tout ensemble fermé, ne séparant pas le plan, de mesure superficielle nulle, contenu dans un angle $O = \{z; | \arg z | \leqq \theta < \frac{\pi}{2}\}$.

Remarquons pour terminer que l'on peut préciser davantage la condition 3.1 lorsque e est suffisamment rare. On a par exemple l'énoncé:

Si e est une partie de l'axe réel positif, et si e est réunion d'intervalles $[a_n, b_n]$ où

$$\lim b_n/a_n = +\infty,$$

posons

$$m(x) = \tfrac{1}{2} \int_{E \cap [1,x]} dt/t,$$

$$M(\sigma) = \sup_n (n\sigma - \log M_n).$$

Alors

$$\int_1^{+\infty} M(\log r)\, e^{-\theta m(r)} dr/r = +\infty$$

est une relation $R^*(e, M_n)$ quelle que soit la constante $\theta > 1$. D'autre part, si l'intégrale converge avec $\theta = 1$, alors $R(e, M_n)$ [et à fortiori $R^*(e, M_n)$], n'est pas vérifiée.

La démonstration de cet énoncé sera donnée dans un autre travail [7].

UNIVERSITÉ DE CAEN (FRANCE).

REFERENCES.

[1] N. Bourbaki, *Topologie générale*, Éléments de Mathématique, Actualité Scientifiques et Industrielles, Paris.

[2]———, *Intégration*, Éléments de Mathématique, Actualités Scientifiques et Industrielles, Paris.

[3] S. Mandelbrojt, *Séries adhérentes*, Paris, 1952.

[4] Mergelyan, "Représentation des fonctions par des séries de polynômes sur des ensembles fermés," *Doklady Akademii Nauk*, Tome 78 (1951), pp. 405-408.

[5] H. Pollard, "On the Bernstein approximation problem," *Proceedings of the American Mathematical Society*, vol. 6 (1955), pp. 402-411.

[6] M. H. Stone, "On the Weierstrass Theorem," *Mathematics Magazine*, vol. 21 (1948). pp. 237-255.

[7] P. Malliavin, "Approximation polynomiale pondérée et produits canoniques," *Comptes Rendus Académie de Paris*, Tome 247 (1958), pp. 2090-2.

ON THE MAXIMALITY OF VANISHING ALGEBRAS.*

By Arthur B. Simon.[1]

Let G be a locally compact Abelian group with invariant Haar measure μ. For any subset S of G, define L_S to be that subset of $L^1(G)$ consisting of all functions whose supports lie in S. When L_S forms an algebra, we call it a vanishing algebra (see [3]). The question naturally arises as to when a vanishing algebra is a maximal subalgebra if $L^1(G)$.

Wermer has proved [4] that if G is a discrete ordered group and S is the set of non-negative elements, then L_S is a maximal proper closed subalgebra of $L^1(G)$ if and only if the ordering in G is Archimedean.

Some time ago, Wermer communicated to me a proof that if G is the real line and S is the right half-line, then L_S is maximal.

In this note, we prove the following converse:

Theorem. *Let S be a measurable subsemigroup of G. If L_S is a maximal proper closed subalgebra of $L^1(G)$, then G is (continuously isomorphic with) either a discrete subgroup of the reals or the real line itself (with S mapping onto the non-negative part).*

Before this theorem was obtained, it seemed quite likely, at least to the author, that Wermer's second theorem (concerning the real line) could be extended to higher dimensional Euclidean space. Now, however, the same construction used in proving our theorem provides a simple example of a proper closed subalgebra which properly contains all those L^1-functions on the plane whose supports lie in the right half-plane.

It is clear that our theorem coupled with Wermer's results give a complete answer as to when a vanishing algebra is a maximal subalgebra.

Throughout this paper we assume that G is a non-trivial additive locally compact Abelian group with invariant Haar measure μ. We also assume G is a measurable set.

* Received November 21, 1958; revised January 14, 1959.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research under contract No. AF 18(600)-1127.

The space $L^1 = L^1(G)$ of all μ-measurable complex valued functions on G with the property that $\int_G |f(x)|\, d\mu(x) < \infty$ forms a Banach Algebra under the norm $\|f\| = \int_G |f(x)|\, d\mu(x)$ with convolution as multiplication. If f is in L^1 and y is any element of G, then f_y, defined by $f_y(x) = f(x-y)$, is again in L^1. We refer to f_y as the "y-translate" of f.

The essence of our theorem is contained in the following two lemmas:

LEMMA 1. *Let H be a measurable semigroup contained in G such that L_H is a maximal proper closed subalgebra of $L^1(G)$. Then $H \cap -H = \{0\}$.*

Proof. Suppose, to the contrary, that H contains an element $t \neq 0$ such that $-t$ is also in H.

For any subset E of G, we have that $((t+E) \cap H') = t + (E \cap H')$; (here H' denotes the set theoretic complement of H). Hence, if E is measurable, then $\mu((t+E) \cap H') = \mu(E \cap H')$.

Since L_H is proper, H' must be a set of positive measure. Pick e_1 in H' such that every open set about e_1 intersects H' in a set of positive measure; the existence of such a point is guaranteed by [3; Lemma 2.2]. Now $e_1 \neq -t + e_1$, so we can find a pre-compact open set E which contains e_1, and whose closure $\bar{E}$ misses $-t + e_1$. Observe that e_1 is an element of the open set $E \cap (t + \bar{E})'$. Therefore $E_0 = E \cap (t + \bar{E})' \cap H'$ is a set of positive finite measure with the property that E_0, $(t + E_0)$, and H are mutually disjoint.

Set $f_+ = \chi_{(t+E_0)}$ ($=$ the characteristic function of the set $(t+E_0)$) and set $f_- = -\chi_{E_0}$; now let $f = f_+ + f_-$. It follows that f is in L^1, $f \neq 0$, and f is not in L_H. It is also true that if y is any element of G, we have

$$\begin{aligned}\int_{H'} f_y(x)\, d\mu(x) &= \int_{H'} f(x-y)\, d\mu(x) \\ &= \int_{H'} \chi_{(t+E_0)}(x-y)\, d\mu(x) - \int_{H'} \chi_{E_0}(x-y)\, d\mu(x) \\ &= \mu[(t + (y+E_0)) \cap H'] - \mu[(y+E_0) \cap H'] = 0.\end{aligned}$$

Consider the closed linear space I consisting of all those L^1-functions g such that for every y in G, $\int_{H'} g_y(x)\, d\mu(x) = 0$. Since, by definition, $(g_y)_z = g_{y+z}$ always holds, it is clear that if g is in I and y is in G, then g_y is also in I. Thus I is an ideal of $L^1(G)$ (see [2; p. 125]). Now I is a non-trivial ideal and I is not contained in L_H because f is in I.

The set of sums $\{I + L_H\}$ is a subalgebra of $L^1(G)$ which properly contains L_H. It is a proper subalgebra since any element in $L^\infty(G)$ which is constant on H' and identically zero on H will annihilate it. This contradiction shows that $H \cap -H = \{0\}$.

LEMMA 2. *Same hypothesis as Lemma 1. Then there is a maximal subsemigroup F_0 of G such that $L_{F_0} = L_H$ and $F_0 \cap -F_0 = \{0\}$.*

Proof. Let $\mathfrak{F} = \{F \subset G\colon F$ is a measurable semigroup, $H \subset F$, and $L_F = L_H\}$. If F is any element of $\mathfrak{F}$, it follows from Lemma 1 that $F \cap -F = \{0\}$. Let F_0 be the union of a maximal tower in $\mathfrak{F}$. Then F_0 is a semigroup and since F_0' contains a set of positive measure, namely $-H$, it follows that L_{F_0} is proper; $L_{F_0} = L_H$.

We claim that F_0 is closed and therefore measurable. For $H + H \subset F_0$, and thus F_0 has a non-empty interior (the sum of two sets of positive measure has a non-empty interior [1]). Pick x not in F_0; then the set of differences $\{x - F_0\}$ is contained in F_0'. Therefore $\bar{F}_0$ is proper and clearly satisfies the conditions of $\mathfrak{F}$. Therefore $F_0 = \bar{F}_0$.

To show F_0 is maximal, let R be any semigroup containing F_0. If $R \neq G$, pick x in R'. Then, as above, $\bar{R}$ is proper and $L_R = L_H$. By the maximality of F_0 in $\mathfrak{F}$, we have $R = F_0$, and Lemma 2 is proved.

Proof of the Theorem. In view of Lemma 2, there is no loss of generality in assuming that S is a maximal semigroup and $S \cap -S = \{0\}$. It follows that $G = S \cup -S$ (see [1; Lemma 4.1]). Let S^0 be the interior of S and S_1 the open semigroup $S^0 - \{0\}$. Let T be any open semigroup which properly contains S_1. If $S' \cap T = \phi$, then $T \subset S^0$, so T must contain 0. If $S' \cap T \neq \phi$, then $-S^0 \cap T \neq \phi$ and 0 is again in T. Thus S_1 is a maximal 0-proper open semigroup, using the terminology of F. B. Wright [5]. Continuing in this vein, the semigroup $s(S_1) = \{x \in G\colon x + S_1 \subset S_1\}$ must be equal to S; for clearly $S \subset s(S_1)$, and since 0 is not in S_1, no element of $-S_1$ is in $s(S_1)$; equality follows because S is maximal. For the same reasons, $s(-S_1) = -S$. Since $S \cap -S = \{0\}$, we know that G is what Wright calls a Hölder group. In the aforementioned paper, it is proved that there is a continuous isomorphism from a Hölder group to the group of reals.

According to the structure theorem for locally compact Abelian groups, we know $G = R^n \oplus G_1$ with $G_1/K = D$, where K is compact, R^n is Euclidean n-space, and D is discrete. The subgroup K must reduce to a point since there are no compact subgroups of the reals. Therefore $G = R^n \oplus D$. If $n \neq 0$, then the image of R^n is connected; hence all of the real line and D

must be just a point. If $n = 0$, then G is discrete and we may also consider the image of G under the isomorphism to be discrete. This completes the proof.

Remarks. (1) We could have assumed that S was a closed subset of G rather than a semigroup since in that case we have proved in [3] that S is the union of a semigroup and a set of measure zero.

(2) In the proof of the theorem, we eliminated the compact group K; i.e. we showed that G contains no non-trivial compact subgroup. We can also prove that in the R^n component, n must be 0 or 1. For, if $n \neq 0$, then D must reduce to a point. Now we have shown that S can be taken to be a maximal, hence closed, semigroup with the property that $S \cap -S = \{0\}$ and $G = S \cup -S$. Clearly, only R^1 contains a subset of this nature.

YALE UNIVERSITY.

REFERENCES.

[1] A. Beck, H. Corson and A. Simon, "The interior points of the product of two subsets of a locally compact group," *Proceedings of the American Mathematical Society*, vol. 9 (1958), pp. 648-652.

[2] L. H. Loomis, *Abstract Harmonic Analysis*, D. Von Nostrand, New York, 1953.

[3] Arthur B. Simon, "Vanishing algebras," to appear in *Transactions of the American Mathematical Society.*

[4] J. Werner, "Subalgebras of group algebras," *Proceedings of the American Mathematical Society*, vol. 6 (1955), pp. 692-694.

[5] Fred B. Wright, "Hölder groups," *Duke Mathematical Journal*, vol. 24 (1957), pp. 567-573.

LINE ELEMENTS ON THE TORUS.*

By Bruce L. Reinhart.[1]

The aim of this paper is to study the relations between the integral curves of a (oriented or nonoriented) line element field on the torus and the homotopy invariants defined by considering it as a map from the torus into the circle. The principal tools are generalizations of the winding number, rotation number, and cycle without contact defined originally by Poincaré [4, pp. 25, 73, 145], and the elementary properties of the first homology group of the torus. Let $F\colon T^2 \to S^1$ be the line element field and F_* the induced map on the first homology group. Then any closed integral curve defines an element of the kernel of F_*. If $F_* \not\equiv 0$, there exists a closed integral curve, the homology class of which generates the kernel. F_* is characterized by a pair of integers (i, j). In case $F_* \not\equiv 0$, the rotation number may be expressed in terms of i and j; in particular, it is always a rational number. A new proof of the classification theorem of Kneser [3] is given, and applied to establish necessary and sufficient conidtions for orientability of a nonoriented line element field, and the best possible homotopically invariant lower bound for the number of closed integral curves. Finally, a few remarks are made about line element fields on the Klein bottle.

1. The winding number on the torus. For the purposes of this paper, we shall consider the torus as the quotient of the (x, y) plane by the lattice of points with integer coordinates. This representation induces in a natural way a parallelization of the torus, which we shall take as fixed throughout. We shall permit ourselves to make changes of coordinates in the plane by integer matrices of determinant one and by translations; such a change induces a one-one map of the torus onto itself which takes parallel vectors into parallel vectors.

We shall concern ourselves with the study of line element fields on the torus; by this we mean C^1 cross sections into the tangent sphere bundle (oriented line elements) or projective space bundle (nonoriented line elements).

* Received October 30, 1958; revised February 24, 1959.

[1] This research was supported by the Office of Naval Research.

Using the canonical parallelization, such a cross section may be considered a map F of the torus T^2 into the sphere S^1 or the projective space P^1. In classical terminology, F is just the Gauss spherical map. A line element field may be represented by a (oriented or nonoriented) vector field, in the sense that at each point the vector is in the direction of the line element assigned; for example, the field of unit vectors with this property. Conversely, any vector field gives rise to a line element field by ignoring the length of the vector and considering only the direction. By this means, we may define the notion of a singular line element field: beginning with a C^1 vector field with isolated zeroes, we construct a line element field defined everywhere except on a set of isolated points.

Let F be a continuous map of T^2 into S^1 and let $F_*: H_1(T^2) \rightarrow H_1(S^1)$ be the induced homology map. By elementary obstruction theory [6, § 34. 6], the homotopy classes of such maps F are in one-one correspondence with the elements of $H^1(T^2; \pi_1(S^1))$, that is, with the maps F_*. The latter maps are characterized by a pair (i, j) of integers such that $F_*(z_1) = iz'$ and $F_*(z_2) = jz'$ where $\{z_1, z_2\}$ is a basis for $H_1(T^2)$ and $\{z'\}$ is a basis for $H_1(S^1)$. By the differentiable approximation theorems [6, § 6. 7], the same holds for C^1 homotopy classes of C^1 mappings.

In order to study the mapping F_*, it is convenient to consider the restriction of F to a closed curve C lying on T^2. By considerations similar to those of the preceding paragraph, it is seen that the homotopy classes of maps of a circle into a circle are determined by a single integer k, called the degree of the map. We may define the winding number $I_F(C)$ of the closed curve C with respect to the field F as the degree of the restriction of F to C. It is independent of admissible coordinate changes in the plane, since the induced map on tangent directions is one-one and orientation preserving, hence is of degree 1. The notion of winding number has been used by numerous authors in studying singularities of a vector field. We shall agree to parametrize S^1 by $\frac{1}{2}\pi$ times the angle between a given vector and the positive x axis, and P^1 by $1/\pi$ times this angle. Then the following proposition relates the various usual definitions of winding number and gives a means of computation. The proposition deals with regular simple closed curves; these are simple closed curves which have everywhere a continuous nonzero tangent vector. Such curves are differentiable submanifolds of class C^1.

PROPOSITION 1. *Let F map the regular simple closed curve C into S^1. Let θ be a parametrization of S^1 by the real numbers modulo 1 and let x_0 be a point of S^1 such that $F^{-1}(x_0)$ is a finite set of points. Let p be the*

number of times that the value x_0 is taken on as θ increases, and n the number of times as θ decreases. Then $k = \int_C F^* d\theta = p - n$.

Proof. The fundamental cycle of C is mapped into k times the fundamental cycle of S^1; hence, the fundamental cocycle of S^1 is mapped into k times the fundamental cocycle of C. But $\int_{S^1} d\theta$ is a representation of the fundamental cocycle of S^1, so $\int_C F^* d\theta$ represents the induced cocycle on C. Hence the latter integral is equal to k as claimed. The points of $F^{-1}(x_0)$ may be divided into three categories according as θ increases, decreases, or attains a local extremum. Let $q_1, \cdots, q_t$ be the set of points of the first two categories, arranged in their natural order on C. Then

$$k = \int_C F^* d\theta = \theta \,\Big|_{F(q_1)}^{F(q_2)} + \cdots + \theta \,\Big|_{F(q_{t-1})}^{F(q_t)} + \theta \,\Big|_{F(q_t)}^{F(q_1)}$$

where θ is to be taken as a real number (not modulo 1). If the two limits of any term are in the first category, the integral is $+1$; if in the second category, -1; and if in different categories, 0. Let p^+ be the number of points in the first category which are followed by a point of the same category, p^- the number of those followed by a point of the second category, n^+ the number of points of the second category which are preceded by a point of the first category, and n^- the number which are preceded by a point of the second category. Then $k = p^+ - n^- = p^+ + (p^- - n^+) - n^- = p - n$.

THEOREM 1. *The winding number of a regular simple closed curve C on T^2 with respect to its oriented tangent vector is ± 1 or zero according as C bounds or not. For the nonoriented case, the numbers are ± 2 or zero respectively.*

Proof. Lift C to a simple arc C' in the plane covering C once. C' is a C^1 curve with nonzero tangent vector, such that the tangents at the two end points are parallel. C' is a closed curve if and only if C bounds; in this case, the winding number of C' in the plane, which clearly equals the winding number on the torus, is well know to be ± 1 [1]. If C does not bound, we construct a regular curve in the plane as follows: Let P' and Q' be the end-points of C', and let l be parallel to $P'Q'$, tangent to C', and such that C' lies entirely on one side of l. Let l meet C' in P, and let PQ be an arc covering C once. Let RS be a line parallel to l and separated from PQ by l. Join PQ to RS by a pair of semicircles tangent to each, thus making a closed curve

$PQSR$. Now the winding number of $PQSR$ with respect to its tangent vector is 1 (respectively -1) while the semicircles each contribute $\frac{1}{2}$ (respectively $-\frac{1}{2}$) to the integral and the line SR contributes nothing. Hence PQ contributes zero; but the integral giving its contribution to the winding number of $PQSR$ clearly gives the winding number of C. Since the canonical map of S^1 onto P^1 is of degree 2, all winding numbers are doubled in that case.

COROLLARY 1. *The homology class defined by a nonbounding closed integral curve of a line element field F lies in the kernel of the homology map F_*. In particular, if F is nonsingular and has a closed integral curve, these conditions are satisfied.*

Proof. The first statement is immediate. If F is nonsingular, no closed integral curve can bound, for the index of such a curve is equal to the total of the indices of the singularities enclosed [1].

COROLLARY 2. *Let C be a nonbounding regular simple closed curve which is tangent to F at a finite number of points. Then $I_F(C) = P - N$, where P is the number of points where F is tangent as the angle increases and N is the number as the angle decreases.*

Proof. Since the winding number of C with respect to its tangent vector is zero, we may deform the map $G_1\colon C \to S^1$ which takes each point of C into the tangent vector at that point into the mapping $G_2\colon C \to 0$. Let $\theta(t)$ be the angle between $(F \mid C)(t)$ and the tangent vector to C at $C(t)$ for some parametrization of C. Then $(F \mid C)(t) = G_1(t) + \theta(t)$. Using the homotopy between G_1 and G_2, we see that $(F \mid C)$ is homotopic to the map $F'\colon C(t) \to \theta(t)$. This map takes on the value 0 only at points of tangency of F with C. Using Proposition 1, Corollary 2 follows immediately.

For the remainder of the paper we shall assume that F is nonsingular. Our immediate goal is to apply our knowledge of $F \mid C$ to derive certain facts about F. Let us first recall a few elementary properties of the first homology group of the torus.

LEMMA 1. *Let $\{\alpha, \beta\}$ form a basis for $H_1(T^2)$* and *let γ be a nonbounding simple closed curve. Then γ is homologous to $m\alpha + n\beta$ with m and n relatively prime; or equivalently, γ may be taken as an element of a new basis $\{\gamma, \gamma'\}$. Moreover, if a connected curve $\tilde{\gamma}$ in the plane covering γ passes through (x_0, y_0), the nearest points on $\tilde{\gamma}$ of the form $(x_0 + i, y_0 + j)$ with i and j integers are $(x_0 + \epsilon m, y_0 + \epsilon n)$, where $\epsilon = \pm 1$. Here we have assumed that α (respectively β) is homologous to the projection of the x (respectively y) axis.*

LEMMA 2. *Let α and α' be simple closed curves on T^2. If they are nonintersecting and nonbounding, then they are homologous. If their intersection number is nonzero, they neither bound nor are homologous.*

Proof. Choose a basis $\{\alpha, \beta\}$ for $H_1(T^2)$; then the intersection number $\alpha \cap \beta = 1$, and $\alpha' \sim m\alpha + n\beta$ with m and n relatively prime. But $\alpha \cap \alpha' = \alpha \cap (m\alpha + n\beta) = n(\alpha \cap \beta) = n$, so $n = 0$ and $m = 1$ as required. The second part follows immediately from the facts that $\gamma \cap \gamma = 0$ and $\gamma \cap \gamma' = 0$ whenever γ' bounds.

THEOREM 2. *If there exists a nonbounding simple closed curve Γ not homologous to a closed integral curve and such that $I_F(\Gamma) = 0$, then $F_* \equiv 0$. In particular, if F has no closed integral curves, these conditions hold.*

Proof. (i) Suppose first F has a closed integral curve C. Since by assumption Γ and C are not homologous, neither is homologous to zero, and each is a simple closed curve contained in the kernel of F_*, it follows by Lemma 1 and elementary properties of the integers that $F_* \equiv 0$.

(ii) Suppose there does not exist a closed integral curve. Then there exists a regular simple closed curve Γ' never tangent to F, such that every semiorbit of F meets Γ' eventually and always crosses Γ' in the same direction [1, p. 416; 5]. Here by semiorbit we mean the curve formed by beginning at an arbitrary point P and following the integral curve through P in one direction. Let P be a point of Γ', and consider a semiorbit through P. This semiorbit must meet Γ' infinitely often. Let Q be a point of accumulation of these intersections and N a flat neighborhood of Q, that is, a neighborhood with coordinates (x, y), $|x| \leqq 1$, $|y| \leqq 1$, such that the integral curves of F in N coincide with the level lines of y. These level lines will be called plaques of N. Since Γ' is never tangent, we may assume N small enough to that the angle between the tangent to Γ' at q and $F(p)$ is greater than ϵ for all p in N and q in $\Gamma' \cap N$. Let N' be a flat subneighborhood of N of such shape that any two plaques in it may be joined into a regular curve which makes an angle less than $\epsilon/2$ with any plaque, and small enough so that $\Gamma_1 = \Gamma' \cap N'$ is connected. Pick Q_1 in Γ_1 and lying on the semiorbit through P. Follow the semiorbit, labeling the successive intersections with Γ' $Q_2, \cdots, Q_{k+1}$, where Q_{k+1} is the next one lying on Γ_1. Q_1 and Q_{k+1} are crossings in the same direction; hence we may join the plaques through them in such a manner as to construct a regular simple closed curve which differs from an integral curve only in N' and which crosses Γ' in the same direction. Call this curve C. The angle between C and F may be

assumed to be less than $\epsilon/2$. By Corollary 2, Γ defines an element of the kernel of F_* because it is never tangent. C defines an element of the kernel because $F \mid C$ differs from the map of C into its tangent vectors by less than $\epsilon/2$, so the maps are deformable into each other. Since C and F cross always in the same direction, the intersection number is nonzero; hence by Lemma 2 neither bounds, and C and F are not homologus. We may then proceed as in case (i) to show that $F_* \equiv 0$. It follows in particular that $I_F(\Gamma) = 0$ for any Γ satisfying the hypotheses of the theorem. This completes the proof.

COROLLARY 3. *If $F_* \not\equiv 0$, F has a closed integral curve.*

Criterion. Suppose there exists a closed curve C such that $I_F(C) \neq 0$. Then F has a closed integral curve. If C' is a nonbounding closed curve not homologous to C and $I_F(C')$ is known, then the homology class of the closed integral curve may be determined by finding the kernel of F_*.

2. Cycles of minimal contact. If F is a fixed line element field and C and C' are two curves which are homotopic by a homotopy which that does not pass through any singular points of F, then $I_F(C) = I_F(C')$. Indeed, the given homotopy induces a homotopy between $F \mid C$ and $F \mid C'$, so the degree of the two maps must be the same. In particular, if F is nonsingular, the winding number $I_F(C)$ depends only upon the homology class of C. Let us set the following problem: Given a homology class on T^2, find a curve in it which is tangent to F at the fewest points. Such a curve will provide the most direct computation of the winding number, by Corollary 2. Throughout the remainder of the paper it will be assumed that F is nonsingular.

Let us fix a homology class which contains a simple closed curve, but does not contain a closed integral curve. This is possible because any two closed integral curves are nonintersecting simple closed curves, so are homologous by Lemma 2.

LEMMA 3. *Let C be a simple closed curve not homologous to a closed integral curve of F or to zero. Then C is homologous to a regular simple closed curve C^* such that:*

(i) *C^* is tangent to F at only a finite number of points.*

(ii) *Every semiorbit of F meets C^* eventually.*

Proof. Recall that F has been assumed nonsingular. Hence at each point we may find a flat coordinate neighborhood. Replace C by a regular curve, also called C, which is homologous to it. Cover C by a finite number

of flat coordinate neighborhoods U_α such that the closure $\bar{U}_\alpha$ is a concentric subsquare in V_α which is also flat. Since C is locally connected, we may at each point of $C \cap \bar{U}_\alpha$ find a neighborhood $W_\beta \subset V_\alpha$ whose intersection with C is connected. Each component of $C \cap \bar{U}_\alpha$ must be covered by a finite number of these, as must the whole set $C \cap \bar{U}_\alpha$; hence this set has finitely many components C_γ. We may cover C by a finite number of the interiors of the sets C_γ; call these sets D_δ and number them consecutively around C from some arbitrary starting point, discarding unnecessary ones.

The lemma may now be proved by induction on δ as follows: D_1 is contained in some $\bar{U}_\alpha$ which contains finitely many of the C_γ. Each C_γ is a connected arc beginning and ending on the boundary of $\bar{U}_\alpha$. Let 2ρ be less than the minimum distance from $\bar{D}_1$ to the other C_γ in $\bar{U}_\alpha$, and describe about D_1 the tube of radius ρ. We shall construct a regular arc lying in the tube and in $\bar{U}_\alpha$, having the same initial and final points and tangent vectors as $\bar{D}_1$, and being tangent to a plaque at only a finite number of points. By the rectifiability of C, we can approximate $\bar{D}_1$ by a finite number of line segments of length less than ρ with endpoints on $\bar{D}_1$; such segments are surely contained in the tube and in $\bar{U}_\alpha$, so do not meet the other C_γ. If any of them lies in a plaque, we may turn it slightly; then $\bar{D}_1$ is approximated by a polygonal arc never lying in a plaque. Finally, we may at each corner smooth out to a regular curve by putting in the arc of a circle. In this way, we get at most one point in each corner where the curve is tangent to a plaque. Special care must be exercised at the endpoints of $\bar{D}_1$; but the same effect may be achieved. In applying this construction to D_2, we actually apply it to that subset of D_2 beginning at the endpoint of $\bar{D}_1$. Proceeding in this manner, statement (i) is proved.

To prove (ii), we consider two cases according as F does or does not have closed integral curves. If it has closed integral curves, they by assumption are not homologous to C^*, hence have nonzero intersection number with it, so must cross it. Any other semiorbit is contained in an annulus formed by cutting the torus along some integral curve. Hence, it must spiral toward some closed integral curve from one side, by the Poincaré-Bendixson theorem [1]. Consequently it also must cross C^*. If F has no closed integral curve, cut T^2 along C^*. If any semiorbit stayed in the annulus thus formed, it would have to spiral toward a closed integral curve; that being excluded, it must meet C^* eventually. This proves Lemma 3.

Lemma 3 justifies the following definition.

Definition. A cycle of minimal contact Γ is a regular simple closed curve,

lying in a given homology class not containing a closed integral curve of F, such that the number of points of tangency is as small as possible. We shall indicate by $\mu(\Gamma)$ the winding number of Γ.

PROPOSITION 2. *Let Γ be a cycle of minimal contact such that $\mu(\Gamma)=0$. Then $F_* \equiv 0$.*

Proof. This follows immediately from Theorem 2.

3. The rotation number. In the classical theory of nonsingular differential equations on the torus, a cycle without contact was much used. We shall use instead a cycle of minimal contact; throughout this section, Γ will denote such a cycle. By use of Γ we shall generalize the classical invariant called the roation number; this invariant will be denoted by $\lambda(\Gamma)$. We shall also find the relation between $\mu(\Gamma)$ and $\lambda(\Gamma)$ on one hand and the integers which characterize F_* on the other. In defining $\lambda(\Gamma)$, we shall assume there exists a closed integral curve, since the contrary case can be handled by known methods [4, 5]. Let us assume we have chosen coordinates in the (x,y) plane so that Γ is homologous to the cycle covered by $x=0$ and passes through the projection of $(0,0)$. Then the inverse image of Γ in the plane contains all the integer points, and each component contains all such points with a fixed x, by Lemma 1. Parametrize Γ differentiably by t, $0 \leqq t \leqq 1$; this induces a parametrization by t, $-\infty < t < \infty$, on all the curves $\tilde{\Gamma}_i$, $i=0, \pm 1, \cdots$, passing through $(i,0)$ and covering Γ, if we understand that $t=0$ at the points $(i,0)$. Let Γ' be the curve covered by $y=0$.

LEMMA 4. *If a semiorbit C' either* (i) *crosses in opposite directions at sucessive points of crossing A and B, or* (ii) *crosses at A and is tangent at B on the side to which it crosses, or* (iii) *is tangent at A and crosses at B from the side on which it is tangent, then the arc AB on C' together with a suitably chosen arc BA on Γ bounds, and contains a point of tangency of Γ with F.*

Proof. Consider the semiorbit from A toward B, and lift it up into one of its connected inverse images $\tilde{C}$ in the plane. We may suppose that A lies on that inverse image $\tilde{\Gamma}$ of Γ which contains $(0,0)$. Now $\tilde{\Gamma}$ and each of its translates separate the plane into two components; hence, if B lay on another inverse image of Γ, C would cross at B in the same direction as at A. Hence, B must also lie on $\tilde{\Gamma}$. The arc AB on $\tilde{\Gamma}$ is well defined, and its projection is the desired arc on Γ. It remains to find a point of tangency. Suppose there is none. Let C' be the closed curve: AB on $\tilde{C}$ followed by BA on $\tilde{\Gamma}$. Let P be the midpoint of AB and consider the semiorbit through P

entering the region bounded by C'. If this semiorbit were to remain inside, there would be a closed integral curve, which would have to bound and hence to surround singular points. Thus the semiorbit leaves at Q. Call whichever of P and Q is closest to A, A_1 and the other, B_1. The curve: A_1B_1 along the semiorbit followed by B_1A_1 along $\tilde{\Gamma}$ will be called C_1'. Continuing in this manner, we construct a series of closed intervals A_iB_i whose intersection is a single point P. P is a point of tangency, for if not there would be a semiorbit entering the interior of C' at P which could not leave again, since its point of leaving must lie on all the arcs A_iB_i of $\tilde{\Gamma}$. Since that is impossible, the lemma is proved.

LEMMA 5. *A semiorbit C of an open integral curve, lifted to $\tilde{C}$ in the plane, crosses the $\tilde{\Gamma}_i$ in the same direction and in monotone order, with possibly a finite number of exceptional crossings. A semiorbit of a closed integral curve C' which is homologous to $m\Gamma + n\Gamma'$ has the property that each covering $\tilde{C}'$ first crosses the curves $\tilde{\Gamma}_{kn}$, $k = \pm 1, \pm 2, \cdots$, in monotone sequence and in the same direction. Similar results hold for the curves $\tilde{\Gamma}_{kn+\alpha}$, with $|kn + \alpha| \geqq |n|$.*

Proof. Since there are a finite number of points of tangency between Γ and F, there are a finite number on C. Let us go far enough on C to be beyond these. If C crosses $\tilde{\Gamma}_i$ twice, it must do so in opposite directions; hence C crosses Γ twice in opposite directions at successive points and marks off an interval D_1 on Γ in which there is a point of tangency. If C reenters the region E_1 bounded by D_1 and a portion of C, there is delineated a subinterval D_{11} on which there is a point of tangency, and C must eventually leave by crossing $D_1 - D_{11}$. If C reenters E_1, it must do so through $D_1 - D_{11}$ and mark off another interval D_{12} on which there is a point of tangency. Since there are a finite number of points of tangency on Γ, C must eventually leave the region E_1 permanently. In a similar manner, a finite number of arcs D_i and regions E_i are defined; when C has passed all these, $\tilde{C}$ must cross the $\tilde{\Gamma}_i$ in monotone sequence as claimed. Now let C' be a closed integral curve, and let $\tilde{C}'$ cover it. Consider a semiorbit starting at (x_0, y_0) on Γ_0. C' passes through $(x_0 + n, y_0 + m)$, but it may meet $\tilde{\Gamma}_n$ first at (x_1, y_1). By periodicity, the first meeting with $\tilde{\Gamma}_{kn}$ will be at $(x_1 + kn, y_1 + km)$. These points are in order on $\tilde{C}'$ because each $\tilde{\Gamma}_{kn}$ separates the plane. The remainder of the lemma is proved similarly.

We shall call a semiorbit positive if eventually the sequence described in Lemma 5 is monotone increasing, and negative if it is monotone decreasing. Note that a given orbit may have two semiorbits of the same sign.

Let P be a point of $\tilde{\Gamma}_0$ and arbitrarily choose one of the semiorbits through it. If this projects into an open semiorbit, choose $i_0 \neq 0$ large enough in absolute value so that the $\tilde{\Gamma}_i$ are crossed in monotone sequence for $|i| > |i_0|$, and set $\phi_i(P)$ to be the t coordinate of the crossing with $\tilde{\Gamma}_i$ for such i. If the semiorbit projects into a closed orbit, put $\phi_i(P)$ equal to the t coordinate of its first crossing with $\tilde{\Gamma}_i$, $i \neq 0$. Then define

$$\lambda'(\Gamma, P) = \lim_{i \to \infty} \phi_i(P)/i.$$

Similarly define $\lambda''(\Gamma, P)$ for the other semiorbit.

LEMMA 6. *$\lambda'(\Gamma, P)$ and $\lambda''(\Gamma, P)$ are equal rational numbers which depend only upon Γ. Moreover, if the closed integral curves belong to the class $m\Gamma + n\Gamma'$, then $\lambda = m/n$.*

Proof. Consider first a closed orbit C, homologous to $m\Gamma + n\Gamma'$. According to our parametrization of $\tilde{\Gamma}_i$, if (x_1, y_1) has parameter t, then $(x_1 + kn, y_1 + km)$ has parameter $t_1 + km$. Hence

$$\lim_{k \to \infty} \phi_{kn}(P)/kn = m/n$$

and similarly for the terms $kn + \alpha$. Hence $\lambda' = \lambda'' = m/n$, and is thus independent of the choice of closed integral curve. But any open orbit is asymptotic to a closed orbit, from which it readily follows that the limit in that case is the same.

Remark. Since m and n are relatively prime, λ and the pair (m, n) determine each other.

Fix the basis $\{\Gamma, \Gamma'\}$ for $H_1(T^2)$ as above. Then the homotopy class of F is defined by the pair of integers (i, j), namely the winding numbers of these basis elements (see § 1).

THEOREM 3. *$\mu(\Gamma) = i$. If $\mu(\Gamma) = 0$, then also $j = 0$. If $\mu(\Gamma) \neq 0$, then $\lambda(\Gamma) = -j/i$.*

Proof. The first statement is obvious, and the second follows from Proposition 2. If $\mu(\Gamma)$ is not zero, there must exist a closed integral curve; let its homology class be $m\Gamma + n\Gamma'$ with m and n relatively prime. We know that this class belongs to the kernel of F_*. Its image under F_* is $mi + nj = 0$, from which we see that $m/n = -j/i$. But by Lemma 6, $\lambda(\Gamma) = m/n$.

4. Classification theorem. In this section we shall apply the cycle of minimal contact to describe qualitatively the integral curves of a nonoriented

line element field. This gives a new proof of a theorem of H. Kneser [3], proved by him by methods of combinatorial topology. We shall deal primarily with the case where there exists a closed integral curve, since the contrary case has been suitably handled elsewhere [2, 5, 7]. By using this classification, we shall prove simple necessary and sufficient conditions for orientability, and give the best possible homotopically invariant lower bound for the number of closed integral curves in terms of homotopy invariants of the field F.

Let us therefore suppose there exists a closed integral curve C, which by change of coordinates may be taken to be homologous to the curve covered by $y = 0$. Let us choose a cycle Γ of minimal contact which is homologous to the cycle covered by $x = 0$. We may suppose that C and Γ meet on the image of $(0, 0)$. Let $\tilde{C}_i$ be that component of the inverse image of C which passes through $(0, i)$ and $\tilde{\Gamma}_i$ similarly for Γ and $(i, 0)$. Then the region bounded by $\tilde{\Gamma}_0$, $\tilde{\Gamma}_1$, $\tilde{C}_0$, and $\tilde{C}_i$ is a fundamental domain, in the sense that it maps onto the torus, and the map is one-one at interior points. Moreover, if C' is an integral curve different from C, there is a component of its inverse image which lies between C_0 and C_1. Let us agree to abbreviate $\mu(\Gamma)$ by μ throughout this section.

LEMMA 7. *Let C' be a semiorbit of an integral curve of F. Then none of the following can occur:*

(i) *C' is tangent to Γ and crosses at the point of tangency.*

(ii) *C' crosses Γ in alternating directions at three crossings in order on C' (not necessarily successive).*

(iii) *C' is tangent to Γ at two points.*

(iv) *C' is tangent from one side and at another crossing goes from that side to the other.*

Proof. (i) If this situation occurs, consider a flat neighborhood N containing just one point of tangency. In N we have a family of plaques, with $\Gamma \cap N$ tangent to one of them at one point. Clearly Γ could be slightly altered in N so as not to be tangent, contradicting its minimal property.

(ii) Let the semiorbit $\tilde{C}'$ in the plane cover C', and suppose for definiteness that the first time $\tilde{C}'$ crosses one of the $\tilde{\Gamma}_i$, it does so from left to right. Let Q be the first crossing from right to left, and $\tilde{P}$ the preceding crossing; both these lie on a particular $\tilde{\Gamma}_i$. If $\tilde{C}'$ again crosses $\tilde{\Gamma}_i$, it mus do so from left to right; let $\tilde{R}$ be the first point where this occurs. If $\tilde{C}'$ does not again cross $\tilde{\Gamma}_i$, it must be a negative semiorbit. In that case, we choose $\tilde{Q}'$ to be

the first point beyond $\tilde{Q}$ where $\tilde{C}'$ crosses from left to right, and $\tilde{P}'$ the next preceding crossing, both lying on $\tilde{\Gamma}_j$. The semiorbit being negative, it must eventually cross $\tilde{\Gamma}_j$ again from right to left; call the first such crossing $\tilde{R}'$. Henceforth, let us drop the primes from the names of these points. Let F_δ (δ positive or negative) be the field constructed form F by rotating through an angle δ. Then the integral curve C_δ of F_δ which passes through $\tilde{Q}$ will pass within a distance ϵ of $\tilde{P}$ and $\tilde{R}$ if $|\delta|$ is small enough. By translation, we may assume that $\tilde{\Gamma}_0$ contans the points $\tilde{P}$, $\tilde{Q}$, and $\tilde{R}$. If $\tilde{Q}$ lies between $\tilde{P}$ and $\tilde{R}$, choose the sign of δ so that C_δ meets $\tilde{\Gamma}_0$ outside the arc $\tilde{P}\tilde{R}$. Replace the arc $\tilde{P}\tilde{R}$ of $\tilde{\Gamma}_0$ by an arc of C_δ, joining so as to form a regular curve $\tilde{\Gamma}'_0$ which is not tangent to F along the newly introduce portion. Likewise define $\tilde{\Gamma}'_i$ for all i. Since the various inverse images of C' do not cross, we may be sure that for δ small enough, the $\tilde{\Gamma}'_i$ do not cross. Hence, their projection Γ' on the torus is a simple closed curve homologous to Γ. By Lemma 4, there are points of tangency on Γ between $\tilde{P}$ and $\tilde{Q}$; since there are none on Γ', the minimal property of Γ is contradicted and the theorem proved for this case. Now suppose $\tilde{R}$ lies between $\tilde{P}$ and $\tilde{Q}$ on $\tilde{\Gamma}_0$. Then there must be another crossing $\tilde{R}_1$. If $\tilde{Q}$, $\tilde{R}$, R_1 are in order on $\tilde{\Gamma}_0$, apply the construction of the first case to them. If not, go on to $\tilde{R}_2$, etc. Now eventually we must come to a situation where the first case can be applied, for if not the semiorbit spirals continually inward, so the limit set would either have to contain or bound a singular point.

(iii) and (iv) are handled similarly to (ii). This proves Lemma 7.

LEMMA 8. *Each closed integral curve C' meets Γ just once and is not tangent at that point.*

Proof. Since the intersection number of C' and Γ is one, they must cross at least once. By Lemma 7, the crossings are not points of tangency. Let $\tilde{P}_0$ on $\tilde{\Gamma}_0$ project into a point of intersection of C' and Γ. Let P_1 on $\tilde{\Gamma}_1$ be a translate of $\tilde{P}_0$ such that both lie on the boundary of a fundamental domain. Then $\tilde{C}'$ enters it at $\tilde{P}_0$ and leaves at $\tilde{P}_1$. If there is more than one point of intersection, examining the arc $\tilde{P}_0\tilde{P}_1$ reveals that one of the forbidden cases in Lemma 7 occurs.

LEMMA 9. *Let P be a point of tangency on Γ. Then the two semiorbits C' and C'' through P have the same sign and each is asymptotic to a closed integral curve. The arc of Γ containing P and bounded by the points of accumulation of the two semiorbits contains just one point of tangency; its interior meets only open integral curves.*

Proof. Neither semiorbit contains another point of tangency, and neither can cross except toward the side on which it is tangent, by Lemma 7. Hence the two semiorbits have thet same sign. Cutting the torus along C, we get an annulus within which C' and C'' stay; hence, by the Poincaré-Bendixson theorem each approaches a closed integral curve from one side. This curve must be homologous to C. These two curves (both may become C when the annulus is rejoined into a torus) mark off an interval I on Γ. No closed integral curve can meet an interior point of I, since it would separate either C' or C'' from the curve to whcih it is asymptotic. Lift I up into the plane and consider the region bounded by the integral curves through its endpoints. This is divided up into a countable number of subregions by the various inverse images of the integral curve through P. Since each other integral curve lies in one of these regions, all are asymptotic to the boundary curves. None of them can be tangent from the opposite direction to the tangent at P, since otherwise (iv) of Lemma 7 would be contradicted. They cannot be tangent from the same direction, since then Lemma 4 would imply that one of the other curves was tangent from the opposite direction. Hence, there are no other points of tangency on I, and the lemma is proved.

LEMMA 10. *Let C' be an open integral curve not lying in one of the regions constructed in Lemma* 10. *Then the two semiorbits are in opposite directions, and are asymptotic to a pair of closed integral curves which bound a region consisting entirely of open integral curves with semiorbits in opposite directions.*

Proof. Each semiorbit is asymptotic to some closed integral curve, which curves we take to bound an interval I as above. If the semiorbits were in the same direction, some integral curve meeting I would have a point of tangency, which case is excluded. Any other semiorbit is also asymptotic to one of the same two closed curves, by the argument used in Lemma 9.

PROPOSITION 3. *Let Γ have μ^+ points of tangency from the left and μ^- from the right. Then the integral curves may be described as follows:*

(i) *There are μ^+ regions bounded by a pair of (possibly not distinct) closed integral curves, such that all integral curves interior to this region are open and have both semiorbits negative.*

(ii) *There are μ^- such regions with both semiorbits positive.*

(iii) *There are certain other regions composed of open integral curves in which the two semiorbits of a given orbit have opposite signs.*

(iv) *The total number of regions described in* (i), (ii), *and* (iii) *is at most countable.*

(v) *If the complement is not the whole space, it is composed entirely of closed integral curves.*

(vi) *If the complement is the whole space, either all integral curves are closed, or all are dense, or the singular case of Poincaré holds.*

Proof. (i), (ii), (iii) and (v) following immediately from the preceding Lemmas 8, 9, and 10. (iv) follows because these regions are disjoint open sets and the torus has a countable base for open sets. (v) in the case where there exists a cycle without contact, which is dealt with in the references given at the beginning of this section. This proves the proposition.

COROLLARY 4. *Let F be a nonoriented line element field. Then F is orientable if and only if i and j are both even.*

Proof. Since the map of S^1 onto P^1 is of degree 2, the necessity is obvious. For the sufficiency, choose a basis for $H_1(T^2)$ as in the classification theorem. Then by Corollary 2, $\mu = \mu^+ - \mu^-$ is even, and so is $\mu^+ + \mu^-$. Hence there are an even number of regions as in (i) and (ii) and the orientation may be carried out in an obvious manner.

COROLLARY 5. *The number of closed integral curves is at least the greatest common divisor of i and j.*

Proof. The number is at least $\mu^+ + \mu^- \geqq |\mu|$. On the other hand, μ may be described as the greatest common divisor of μ and 0, and the notion of greatest common divisor is invariant under change of basis in $H_1(T^2)$.

5. The Klein bottle. The tangent sphere bundle of the Klein bottle K^2 is not a product, but the tangent projective bundle is. Hence, we may consider nonoriented line element fields as maps $F: K^2 \to P^1$, and define winding numbers as for the torus. The homotopy classes of such maps are determined by the induced homology maps $F_*: H_1(K^2) \to H_1(P^2)$. Since the former group is isomorphic to the direct sum of the integers and the integers modulo 2, these maps are determined by a single integer i which tells how often the free generator covers P^1. Using the covering of the Klein bottle by the torus and the fact that every element of the fundamental group of the Klein bottle is of infinite order, we show that the winding number of a simple closed curve is zero if and only if it is not nullhomotopic. Thus, if F is nonsingular, there can be no closed integral curve which is nullhomotopic.

If an integral curve is homologous to the generator of order 2, cutting along it gives rise to a plane annulus; thus we may show that any other closed integral curve is homologous to it. On the other hand, if $F_* \not\equiv 0$, this is the only homology clas that can contain a closed integral curve. We have proved the following proposition:

PROPOSITION 4. *Let F be a nonoriented line element field on K^2 such that $F_* \not\equiv 0$. Then the only possible closed integral curves are homologous to the generator of order 2 of $H_1(K^2)$.*

Remark. By a theorem of Kneser [3], every line element field on the torus has a closed integral curve. The author would like to see a non-combinatorial proof of the latter theorem.

THE UNIVERSITY OF MICHIGAN.

REFERENCES.

[1] E. A. Coddington and N. Levinson, *Theory of ordinary differential equations*, New York, 1955.

[2] A. Denjoy, "Sur les courbes définies par les équations différentielles à la surface du tore," *Journal de Mathématiques Pures et Appliquées* (9), vol. 11 (1932), pp. 333-375.

[3] H. Kneser, "Reguläre Kurvenscharen auf den Ringflächen," *Mathematische Annalen*, vol. 91 (1923), pp. 135-154.

[4] H. Poincaré, *Oeuvres*, vol. i, Paris, 1928.

[5] C. L. Siegel, "Note on differential equations on the torus," *Annals of Mathematics* (2), vol. 46 (1945), pp. 423-428.

[6] N. E. Steenrod, *The topology of fibre bundles*, Princeton, 1951.

[7] E. R. van Kampen, "The topological transformations of a simple closed curve into itself," *American Journal of Mathematics*, vol. 57 (1935), pp. 142-152.

NOTE ON FORMAL LIE GROUPS.*[1]

By SHIGEAKI TÔGÔ.

---

1. Non-commutative formal Lie groups over an algebraically closed field are investigated by J. Dieudonné [3] by considering the homomorphisms of a formal Lie group G into linear groups. When such homomorphisms are injective, the algebraic hull $\mathfrak{A}(G)$ of the image of G by such a homomorphism is defined. Among his results, he asked the questions about the relations between the algebraic hull $\mathfrak{A}(S)$ of a maximal solvable subgroup S (resp. a maximal torus, a Cartan subgroup) of G and a maximal solvable connected subgroup (resp. a maximal torus, a Cartan subgroup) of $\mathfrak{A}(G)$ and between the center of S and that of G, and he also asked whether the l. u. b. of maximal solvable subgroups (resp. Cartan subgroups) of any formal Lie group H is equal to H. It is the purpose of this note to answer these questions and to present some other results on formal Lie groups.

The author wishes to express his thanks to Professor J. Dieudonné for his valuable comments in preparing this note.

2. A formal Lie group G of dimension n over a field K of arbitrary characteristic consists in giving n formal series without constant terms and with coefficients in K in two systems of n indeterminates satisfying the conditions which correspond to the usual condition on the identity and the associative law. Although it is not set-theoretic, all notions corresponding to the set-theoretic notions in groups are introduced into G [3, Chap. I and II]. Through this note we assume that the basic field K is algebraically closed.

We shall recall some of the definitions, results and notations on formal Lie groups given in [3, Chap. III]. We can associate a formal Lie group H^* to any algebraic group H. A formal Lie group G is called *representable* if it is isogenous to a subgroup of the formal Lie group $GL^*(n,K)$ associated to the general linear group $GL(n,K)$. Then the algebraic hull $\mathfrak{A}(G)$ of the image of G by the injective homomorphism of G into $GL^*(n,K)$ can be

---

* Received November 21, 1858; revised January 14, 1959.

[1] Research supported by the National Science Foundation.

defined. We do not recall the definition. $\mathfrak{A}(G)^*$ is denoted by $\mathfrak{A}^*(G)$. $\mathfrak{A}(G)$ is solvable (resp. nilpotent, commutative) if and only if G is solvable (resp. nilpotent, commutative). If M, N are subgroups of $GL^*(n,K)$ and if M centralizes (resp. normalizes) N, then $\mathfrak{A}(M)$ centralizes (resp. normalizes) $\mathfrak{A}(N)$. It is known that $DG = \mathfrak{A}^*(DG) = D(\mathfrak{A}(G))^*$. If H is a connected algebraic group, then $\mathfrak{A}(H^*) = H$. Let f be a rational homomorphism of H into an algebraic group H_1. Then there exists a corresponding homomorphism $\boldsymbol{f}$ of H^* into $H_1{}^*$ and $\boldsymbol{f}(H^*) = f(H)^*$. If N is the kernel of f, then N^* is the kernel of $\boldsymbol{f}$. For an element s of H, $\boldsymbol{a}_s$ denotes the automorphism of H^* corresponding to the inner automorphism of H induced by s. The subgroups of any formal Lie group form a complete lattice. For its subgroups G_1, G_2, we denote by $G_1 \wedge G_2$, $G_1 \vee G_2$ the g. l. b. and the l. u. b. of G_1 and G_2. If, for algebraic subgroups H_1, H_2 of $GL(n,K)$, we denote by $H_1 \vee H_2$ the smallest algebraic subgroup of $GL(n,K)$ containing H_1, H_2, then we have $(H_1 \vee H_2)^* = H_1{}^* \vee H_2{}^*$.

3. We first prove the following

THEOREM 1. *Let G be a representable formal Lie group over an algebraically closed field of arbitrary characteristic. If S_1, S_2 are maximal solvable subgroups (resp. maximal tori, Cartan subgroups) of G, then there exists an element s of $\mathfrak{A}(DG)$ such that $\boldsymbol{a}_s(S_1) = S_2$.*

In order to prove this theorem, it suffices to use the following lemma instead of the conjugation theorem by A. Borel in the proofs of [3, Prop. 31 a), Prop. 34 a) and Cor. of Prop. 39].

LEMMA. *Let G be a connected algebraic linear group. If R_1, R_2 are maximal solvable connected subgroups (resp. maximal tori) of G, then there exists an element s of $D^\infty G$ (resp. $C^\infty G$) such that $s^{-1}R_1 s = R_2$.*

Let f be a rational homomorphism of G with $D^\infty G$ as its kernel [2, p. 119]. Then $f(R_1)$ is a maximal solvable connected subgroup of $f(G)$ [1, (22.3)]. Since $f(G)$ is solvable and connected, we have $f(G) = f(R_1)$ and therefore

$$G = R_1(D^\infty G). \tag{1}$$

Let g be the natural mapping of G onto G/R_2. G/R_2 is a projective variety and G operates on G/R_2. Then it is known [1, (15.7)] that R_1 admits a fixed point, which shows that there exists an element s of G such that $R_1 s R_2 = s R_2$, i. e. $s^{-1}R_1 s \subset R_2$. By the maximality of R_1 we have $s^{-1}R_1 s = R_2$.

By virtue of the formula (1) s can be taken in $D^\infty G$. The statement for maximal tori follows from the one for maximal solvable connected subgroups and [1, (12.9)].

As an answer to the first question in 1, we shall prove

THEOREM 2. *Let G be a representable formal Lie group over an algebraically closed field of arbitrary characteristic. If S is a maximal solvable subgroup (resp. a maximal torus, a Cartan subgroup) of G, then $\mathfrak{A}(S)$ is a maximal solvable connected subgroup (resp. a maximal torus, a Cartan subgroup) of $\mathfrak{A}(G)$, and conversely.*

It suffices to prove the theorem when G is a subgroup of $GL^*(n,K)$. Let R be a maximal solvable connected subgroup of $\mathfrak{A}(G)$ containing $\mathfrak{A}(S)$. Take a rational homomorphism f of $\mathfrak{A}(G)$ with $D(\mathfrak{A}(G))$ as its kernel [2, p. 119]. Then $f(R)$ is a maximal solvable connected subgroup of $f(\mathfrak{A}(G))$ [1, (22.3)] and therefore $f(R)=f(\mathfrak{A}(G))$. Let $\mathfrak{f}$ be the corresponding homomorphism of $\mathfrak{A}^*(G)$. Then the kernel of $\mathfrak{f}$ is $(D\mathfrak{A}(G))^*=DG$ and we have $\mathfrak{f}(R^*)=f(R)^*$, $\mathfrak{f}(\mathfrak{A}^*(G))=f(\mathfrak{A}(G))^*$. Therefore we have $\mathfrak{f}(R^*)=\mathfrak{f}(\mathfrak{A}^*(G))$ and $\mathfrak{A}^*(G)=R^*\vee DG$. Then we assert that $G=(R^*\wedge G)\vee DG$. In fact, it is clear that $(R^*\wedge G)\vee DG$ is a subgroup of G. Since DG is a normal subgroup of $\mathfrak{A}^*(G)$, by [3, Prop. 11] we have

$$\dim \mathfrak{A}^*(G)=\dim R^*+\dim DG-\dim(R^*\wedge DG).$$

From the facts that $\mathfrak{A}^*(G)=R^*\vee G$ and that G is normal in $\mathfrak{A}^*(G)$, it follows that

$$\dim \mathfrak{A}^*(G)=\dim R^*+\dim G-\dim(R^*\wedge G).$$

Therefore

$$\begin{aligned}\dim G&=\dim(R^*\wedge G)+\dim DG-\dim(R^*\wedge DG)\\&=\dim((R^*\wedge G)\vee DG),\end{aligned}$$

whence we have $G=(R^*\wedge G)\vee DG$, as was asserted. Since $R^*\wedge G$ is a solvable subgroup of G containing S, we have $S=R^*\wedge G$ and

$$G=S\vee DG. \tag{2}$$

Then it is clear that $\mathfrak{A}(G)=\mathfrak{A}(S)\vee\mathfrak{A}(DG)$ and therefore $\mathfrak{A}^*(G)=\mathfrak{A}^*(S)\vee DG$. Since $\mathfrak{A}^*(S)\subset R^*$, we have also $\mathfrak{A}^*(G)=Ro\vee DG$. By using these formulas where DG is normal in $\mathfrak{A}^*(G)$, it is easy to see that

$$\dim R^*=\dim\mathfrak{A}^*(S)+\dim(R^*\wedge DG)-\dim(\mathfrak{A}^*(S)\wedge DG).$$

Since $\mathfrak{A}^*(S) \vee (R^* \wedge DG) \subset R^*$ and $R^* \wedge DG$ is normal in R^*, we have

$$\dim R^* = \dim(\mathfrak{A}^*(S) \vee (R^* \wedge DG))$$

and $R^* = \mathfrak{A}^*(S) \vee (R^* \wedge DG)$. Then we have $R^* = \mathfrak{A}^*(S)$ and therefore $R = \mathfrak{A}(S)$. Conversely, let R_1 be any maximal solvable connected subgroup of $\mathfrak{A}(G)$. If we put $S_1 = G \wedge R_1^*$, then $\mathfrak{A}(S_1) \subset \mathfrak{A}(R_1^*) = R_1$. But S_1 is a maximal solvable subgroup of G by [3, Prop. 31 b)]. Therefore it follows from the direct part that $R_1 = \mathfrak{A}(S_1)$.

Let T be a maximal torus of G and let S be a maximal solvable subgroup of G containing T. Then $\mathfrak{A}(T)$ is a maximal torus of $\mathfrak{A}(S)$ [3, Cor. of Prop. 38]. As is shown above, $\mathfrak{A}(S)$ is a maximal solvable connected subgroup of $\mathfrak{A}(G)$. Therefore $\mathfrak{A}(T)$ is a maximal torus of $\mathfrak{A}(G)$ [1, (16.10)]. The converse part follows from the direct part and [3, Prop. 34 b)].

Let C be a Cartan subgroup of G, i.e. the centralizer $\mathfrak{Z}(T)$ of a maximal torus T in G. Then $\mathfrak{A}(T)$ is a maximal torus of $\mathfrak{A}(G)$. Denote by H the centralizer of $\mathfrak{A}(T)$ in $\mathfrak{A}(G)$. Then H is a Cartan subgroup of $\mathfrak{A}(G)$ [1, (20.4)]. Since $\mathfrak{A}(C)$ centralizes $\mathfrak{A}(T)$, it is clear that $\mathfrak{A}(C) \subset H$. As in the first part of the proof, by considering a rational homomorphism of $\mathfrak{A}(G)$ with $D\mathfrak{A}(G)$ as its kernel, we have $\mathfrak{A}^*(G) = H^* \vee DG$,

$$G = C \vee DG, \tag{3}$$

and then $\mathfrak{A}(C) = H$. Conversely let H_1 be any Cartan subgroup of $\mathfrak{A}(G)$. Then by [1, (20.4)] H_1 is the centralizer of a maximal torus Q of $\mathfrak{A}(G)$. By the statement for a maximal torus, we have $Q = \mathfrak{A}(T_1)$, where T_1 is a maximal torus of G. Put $C = \mathfrak{Z}(T_1)$. Then it follows from the direct part that $H_1 = \mathfrak{A}(C)$. Thus the proof is complete.

From the theorem we have thet following corollaries the first one of which answers the second question in 1.

COROLLARY 1. *Let S be a maximal solvable subgroup of G. Then the center $Z(S)$ of S is equal to the center $Z(G)$ of G.*

By Theorem 2, $\mathfrak{A}(S)$ is a maximal solvable connected subgroup of $\mathfrak{A}(G)$. Therefore $Z(\mathfrak{A}(S)) = Z(\mathfrak{A}(G))$ by [1, (18.5)]. Then we have $Z(\mathfrak{A}^*(S)) = Z(\mathfrak{A}^*(G))$ by [3, Prop. 21]. But we have $Z(S) = G \wedge Z(\mathfrak{A}^*(S))$. Indeed, it is clear that $\mathfrak{A}(S)$ centralizes $\mathfrak{A}(Z(S))$. Then $\mathfrak{A}^*(S)$ centralizes $\mathfrak{A}^*(Z(S))$ and therefore $Z(S)$. It follows that $Z(S) \subset G \wedge Z(\mathfrak{A}^*(S))$. The inverse inclusion is evident. In a similar way it can be verified that $Z(G) = G \wedge Z(\mathfrak{A}^*(G))$. Therefore we have $Z(S) = Z(G)$, completing the proof.

COROLLARY 2. *G is a formal Lie group associated to an algebraic group*

(i) *if and only if a maximal solvable subgroup is associated to an algebraic group;*

(ii) *if and only if a Cartan subgroup is associated to an algebraic group.*

If a maximal solvable subgroup S of G is associated to an algebraic group, then $S=\mathfrak{A}^*(S)$. Using the formula (2) in the proof of Theorem 2, we have

$$G=S\vee DG=\mathfrak{A}^*(S)\vee\mathfrak{A}^*(DG)=(\mathfrak{A}(S)\vee\mathfrak{A}(DG))^*.$$

The converse is evident. The second part can be verified in a similar way by using the formula (3) in the proof of Theorem 2.

The following theorem is an answer to the third question in 1.

THEOREM 3. *Let G be a formal Lie group over an algebraically closed field of characteristic $p>0$. Then the* l. u. b. *of maximal solvable subgroups (resp. Cartan subgroups) of G is equal to G.*

Put $G'=G/Z(G)$. Then G' is representable [3, Prop. 20]. Let f be the natural epimorphism of G onto G'. Then we have $f(DG)=DG'$ [3, Cor. of Prop. 16]. Let S be a maximal solvable subgroup of G. Then $f(S)$ is a maximal solvable subgroup of G' [3, p. 375]. By the formula (2) in the proof of Theorem 2 we know that $G'=f(S)\vee DG'$. Therefore we have $f(S\vee DG)=G'$. Since $Z(G)\subset S$, we have $G=S\vee DG$. Denote by G_1 the l. u. b. of maximal solvable subgroups of G. As is shown in [3, p. 376], owing to a result of A. Borel, the l. u. b. of maximal solvable subgroups of G' contains $D(G')$. Therefore G_1 contains DG and we have $G_1=G$.

Let T be a maximal torus of G and put $T'=f(T)$. Then it is known that T' is a maximal torus of G' [3, p. 379]. Put $C=\mathfrak{Z}(T)$. Then $f(C)$ is contained in $\mathfrak{Z}(T')$. It is clear that $f^{-1}(\mathfrak{Z}(T'))$ is nilpotent and contains C. By the maximality of C we have $C=f^{-1}(\mathfrak{Z}(T'))$ and therefore $f(C)=\mathfrak{Z}(T')$, i. e. $f(C)$ is a Cartan subgroup of G'. By the formula (3) in the proof of Theorem 2 we know that $G'=f(C)\vee DG'$. Therefore we have $f(C\vee DG)=G'$. Since C contains $Z(G)$, we have $G=C\vee DG$. It is now easy to conclude that the l. u. b. of Cartan subgroups of G is equal to G.

4. By [3, Cor. 2 of Prop. 9 and Prop. 11c)] and the chain conditions we see that the l. u. b. N of all solvable normal subgroups of a formal Lie group G is the largest solvable normal subgroup of G. We call N the *radical* of G.

G is called *semi-simple* if the radical of G is equal to e (cf. [3, p. 385]). We shall prove the following

THEOREM 4. *Let G be a representable formal Lie group over an algebraically closed field of arbitrary characteristic and let N be the radical of G. Then $\mathfrak{A}(N)$ is the radical of $\mathfrak{A}(G)$, and $G \wedge \mathfrak{A}^*(N) = N$.*

It is clear that $\mathfrak{A}(N)$ is a solvable normal subgroup of $\mathfrak{A}(G)$. Therefore, if we denote by M the radical of $\mathfrak{A}(G)$, then $\mathfrak{A}(N)$ is contained in M. Let f be a rational homomorphism of $\mathfrak{A}(G)$ with M as its kernel. Then $f(\mathfrak{A}(G))$ is a connected semi-simple algebraic group. By using the results of C. Chevalley that any connected semi-simple algebraic group is equal to its derived subgroup, we have

$$f(D^\infty \mathfrak{A}(G)) = D^\infty f(\mathfrak{A}(G)) = f(\mathfrak{A}(G)).$$

The rest of the proof of the first part of the theorem runs exactly parallel to the corresponding part in the proof of Theorem 2. It can therefore be omitted. We only note that, coresponding to the formulas (2) and (3), we have

$$G = N \vee D^\infty G. \tag{4}$$

the second part is evident.

COROLLARY 1. *A representable formal Lie group is associated to an algebraic group if and only if so is the radical.*

This can be proved in the same manner as in the proof of Corollary 2 of Theorem 2, by making use of the formula (4).

Furthermore, the fact stated in [3, Th. 7] is another consequence of the theorem. Namely we have

COROLLARY 2. *If G is a semi-simple formal Lie group, then G is isogenous to a group H^* where H is a semi-simple algebraic group, and conversely.*

If G is a semi-simple Lie group, then $Z(G) = e$ and therefore G is representable. There exists an isogenous homomorphism $\boldsymbol{u}$ of G such that $\boldsymbol{u}(G)$ is a subgroup of $GL^*(n, K)$. It now follows from Corollary 1 that $\boldsymbol{u}(G) = H^*$ where H is an algebraic group. By the above theorem it is obvious that the radical of H is equal to e, i.e. H is semi-simple. Conversely, suppose that H' is a connected semi-simple algebraic group. If N is the

radical of H'^*, then $\mathfrak{A}(N)$ is the radical of H' since $\mathfrak{A}(H'^*) = H'$. Therefor $\mathfrak{A}(N) = e$, whence $N = e$, i.e. H'^* is semi-simple, completing the proof.

HIROSHIMA UNIVERSITY
AND
NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956), pp. 20-82.

[2] C. Chevalley, *Théorie des groupes de Lie*, Tome III, Paris, 1955.

[3] J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ (VI)." *American Journal of Mathematics*, vol. 79 (1957), pp. 331-388.

ON SEMISIMPLICIAL FIBRE-BUNDLES.*

By M. G. BARRATT,[1] V. K. A. M. GUGENHEIM [2] and J. C. MOORE.[1]

I. 1. Introduction. The intent of this paper is to begin the study of semisimplicial fibre bundles, and to show how general fibre bundles are. The semisimplicial analogue of a fibre space of the type defined by Serre has been known for several years now, and it has been realized that if one replaced a geometric fibre map of this type by the associated map of the singular complex of the total space into the singular complex of the base one obtains a semisimplicial fibre map, or Kan fibre map. However, one can go much further. Here, given a Kan fibre map, we first choose a "minimal fibre map" (cf. II. 2) which is a fibre-wise deformation retract of the original fibre map, and then proceed to show that this minimal fibre map is in fact the map of the total complex of a semisimplicial fibre bundle into the base complex.

In the description of a semisimplicial fibre-bundle with fibre Y there occurs a certain group-complex $A(Y)$ or, more generally, one of its subgroups Γ; the consequential notion "Γ-bundle" is the semisimplicial analogue of a Steenrod fibre bundle with structural group Γ (see the definitions in IV. 2. 4); in particular the classical notions of the associated principal bundle and the classifying space reappear in our theory (IV. 4. 3, 4. 4, 5. 6).

Applications of this theory to the relationship between fibre-bundles and fibre-space (in the classical sense), and to the homology theory of fibre-spaces, will be treated elsewhere.

I. 2. Terminology. The terminology and theory of semisimplicial complexes (cf. [1], for instance) will be taken for granted; "complex" and "map" will mean "complete semisimplicial complex" and "complete semisimplicial map" respectively. The symbol 1 will denote the identity (in many contexts), the unit element in certain groups, as well as an object described in II. 2 below.

* Received September 19, 1958.

[1] Barratt and Moore were partially supported by the Air Force Office of Scientific Research of the Air Research and Development Command under Contract No. AF 18 (600)-1494.

[2] Gugenheim was partially supported by and this report is issued under Contract No. DA-36-034-ORD-2588RD of the Department of the Army, Office of Ordnance Research.

II. Apparatus. This chapter is purely technical and deals mostly with the treatment of homotopies in complexes; cf. [2] for more details.

1. Models. The n-simplex Δ^n is, for our purposes, best defined as follows: Let δ^n be a "generator" in dimension n; Δ^n is the set of all elements $\phi\delta^n$, where ϕ is a semisimplicial operator with domain-dimension n.

We shall write

$$\delta^n{}_i = \partial_0 \cdots \partial_{i-1}\partial_{i+1} \cdots \partial_n \delta^n \epsilon \Delta^n{}_0$$

and call it the "i-th vertex."

Let X be any complex. We shall frequently identify the element $x \in X_n$ with the map $x: \Delta^r \to X$ defined by $x(\phi\delta^n) = \phi x$; in particular we define

$$\epsilon^i = \partial_i \delta^n : \Delta^{n-1} \to \Delta^n, \qquad \eta^i = s_i \delta^n : \Delta^{n+1} \to \Delta^n.$$

In Δ^n we define a "contraction operator" D by

$$D\phi\delta^n = \phi' s_0 \delta^n,$$

where ϕ' is obtained from ϕ by increasing all subscripts by 1. We have

$$(1) \qquad \begin{aligned} \partial_0 D &= \text{identity}, \\ \partial_{i+1} D &= D\partial_i \text{ in dimension } > 0, \\ \partial_1 Dx &= \delta^n{}_0 \text{ if } x \in \Delta^n{}_0, \\ D\delta^n{}_0 &= s_0 \delta^n{}_0. \end{aligned}$$

Definition. We call a complex B simplicially contractible (to b_0) if there is an operator D satisfying (1) with $\delta^n{}_0$ replaced by b_0.

2. Prisms. We write $I = \Delta^1$; also, it will be convenient to denote δ'_0, δ'_1 and all their degeneracies by 0, 1 respectively.

Let A be a complex; by $A_{r,n}$ we denote the set of all maps $u: I^r \times \Delta^r \to A$ (where $I^1 = I$, $I^{r+1} = I \times I^r$). In an evident manner we can define operators

$$\begin{aligned} \partial_i &: A_{r,n} \to A_{r,n-1} && (0 \leqq i \leqq n), \\ s_i &: A_{r,n} \to A_{r,n+1} && (0 \leqq i \leqq n), \\ \lambda^\epsilon{}_j &: A_{r,n} \to A_{r-1,n} && (\epsilon = 0, 1, 1 \leqq j \leqq r), \\ \sigma_j &: A_{r,n} \to A_{r+1,n} && (1 \leqq j \leqq r+1), \end{aligned}$$

where we identify $A_{0,n}$ and A_n in the obvious way; the operators $\lambda^\epsilon{}_j$ are obtained by taking the face $\epsilon_{1-\epsilon}$ in the j-th factor; the ∂_i, s_i satisfy the usual relations; the $\lambda^\epsilon{}_j$, σ_j satisfy the corresponding identities of the well-known "semicubical theory"; finally, "simplicial" and "cubical" operators commute.

There are also "simplicial subdivisionoperators"

$$S_i\colon A_{r,n} \to A_{r-1,n+1} \qquad (0 \leqq i \leqq n)$$

satisfying certain identities (cf. [2], [3]); an element $u \in A_{r,n}$ is completely determined by the elements $S_i u$.

3. Homotopies.

3.1. Lemma. *Let $f_0, f_1\colon A \to B$ be maps. The following two statements are equivalent:*

(i) *There is a map $F\colon I \times A \to B$ such that*

$$F(0,x) = f_0(x), \qquad F(1,x) = f_1(x).$$

(ii) *There is an operator $U\colon A_q \to B_{1,q}$ $(q \geqq 0)$ such that*

$$\lambda^0{}_1 U = f_0, \qquad \lambda^1{}_1 U = f_1, \qquad \partial_i U = U \partial_i, \qquad s_i U = U s_i.$$

In fact, we define

$$U(x)(\phi\delta^1, \psi\delta^q) = F(\phi\delta^1, \psi x),$$
$$F(\phi\delta^1, x) = U(x)(\psi\delta^1, \delta^q),$$

where ϕ, ψ are semisimplicial operators.

Definition. In the situation of 3.1 we call f_0, f_1 homotopic, F or U a homotopy.

If B is a Kan complex, homotopy is an equivalence relation.

Note. In questions of homotopy, we shall usually use the "classical" form (i) in the statements of our propositions; nearly always, however, it is the form (ii) that is best used in the proofs.

We say that a space B is contractible (to b_0) if the maps $1\colon B \to B$ and $B \to b_0 \in B_0$ are homotopic; this means that there is a homotopy $H\colon B \to B$ such that

$$\lambda^1{}_1 H = 1,$$
$$\lambda^0{}_1 H x = s^q{}_0 b_0 \quad \text{if} \quad x \in B_q,$$
$$\partial_i H = H \partial_i,$$
$$s_i H = H s_i,$$
$$H b_0 = \sigma_1 b_0.$$

It is easily proved (using the operators S_i!) that if a space is simplicially contractible, then it is contractible.

III. Fibre Maps.

1. Terminology. A map $p: E \to B$ will be denoted by (E, B, p) and a commutative diagram

$$\begin{tikzcd} E' \arrow[r, "\bar{f}"] \arrow[d, "p'"] & E \arrow[d, "p"] \\ B' \arrow[r, "f"] & B \end{tikzcd}$$

by $(\bar{f}, f): (E', B', p') \to (E, B, p)$; we refer to $(\bar{f}, f)$ as a map.

Two maps $(\bar{f}_0, f_0)$, $(\bar{f}_1, f_1): (E', B', p') \to (E, B, p)$ will be said to be *homotopic* if there is a map $(\bar{F}, F): (I \times E', I \times B', 1 \times p') \to (E, B, p)$ such that $\bar{F} \mid 0 \times E' = \bar{f}_0$, $\bar{F} \mid 1 \times E' = \bar{f}_1$ (with a slight abuse of language!), and similarly for F. If $f_0 = f_1 = f$ and $F = fp_2$, where $p_2: I \times B \to B$ is the projection, then we say that $(\bar{f}_0, f)$ and $(\bar{f}_1, f)$ are homotopic *rel. f*.

Homotopy is alternatively expressed by the existence of $\bar{U}: E'_n \to E_{1,n}$, $U: B'_n \to B_{1,n}$ $(n \geqq 0)$ such that $p\bar{U} = Up'$ and $\lambda^0{}_1\bar{U} = \bar{f}$, $\lambda^1{}_1 U = \bar{f}_1$, $\lambda^0{}_1 U = f_0$, $\lambda^1{}_1 U = f_1$. The homotopy is rel. f if $U = \sigma_1 f$.

If there are maps $(\bar{f}, f)$ and $(\bar{g}, g)$ such that $(\bar{f}\bar{g}, fg)$, $(\bar{g}\bar{f}, gf)$ are homotopic to $(1, 1)$, then we call either a *homotopy equivalence*; if $f = g =$ identity on B, and the two homotopies are rel. this identity, then we refer to a *strong* homotopy equivalence; in particular we have the notion of *homotopy retraction* and *strong homotopy retraction.*

2. Definition. (E, B, p) will be called a *fibre-map* if p is onto and for $n > 0$ satisfies the following condition:

Given an integer t, $0 \leqq t \leqq n$, $e_i \in E_{n-1}$ for all i, $0 \leqq i \leqq n$, $i \neq t$, and $b \in B_n$ such that

$$\partial_i e_j = \partial_{j-1} e_i \qquad (i < j, i, j \neq t),$$

$$p e_i = \partial_i b \qquad (i \neq t),$$

then there is $e \in E_n$ such that

$$e_i = \partial_i e \qquad (i \neq t),$$

$$b = pe.$$

If, further, $\partial_t e$ depends on the e_i and b only, then (E, B, p) is said to be a *minimal* fibre-map.

3. Homotopy covering and lifting theorems.

3.1. LEMMA. *Let $L = 0 \times \Delta^{n-1} \cup I \times \dot{\Delta}^{n-1} \subset I \times \Delta^{n-1}$, let (E, B, p) be a fibre-map and*

$$\bar{F}: I \times \Delta_{n-1} \to B,$$
$$F_0: L \to E$$

be such that $pF_0 = \bar{F} \mid L$.

Then F_0 has an extension $F: I \times \Delta^{n-1} \to E$ such that $pF = \bar{F}$.

If (E, B, p) is minimal, $F \mid 1 \times \Delta^{n-1}$ is unique.

In other words (cf. 2.2), *given $e_i \in E_{1,n-1}$ $(n > 0, 0 \leqq i \leqq n)$, $e^0{}_1 \in E_n$, $b \in B_{1,n}$ such that*

$$\partial_i e_j = \partial_{j-1} e_i \qquad (i < j),$$
$$\lambda^0{}_1 e_i = \partial_i e^0{}_1,$$
$$pe_i = \partial_i b, \qquad pe^0{}_1 = \lambda^0{}_1 b,$$

then there is $e \in E_{1,n}$ such that

$$e_i = \partial_i e, \qquad e^0{}_1 = \lambda^0{}_1 e, \qquad pe = b.$$

If p is minimal, $\lambda^1{}_1 e$ is unique. The roles of $\lambda^0{}_1$, $\lambda^1{}_1$ can be exchanged.

This is a special case of Theorem 3* in [2], except for the addendum which follows easily from the argument there given.

3.2. Covering homotopy extension theorem. *In the commutative diagram $(\bar{f}, f): (E', B', p) \to (E, B, p)$, det p be a fibre-map, let $A' \subset B'$ be a subcomplex (possibly empty!) and $G' = p'^{-1} A' \subset E'$.*

Let maps

$$H: I \times B' \to B,$$
$$\bar{h}: I \times G' \to E$$

be given such that

$$H(0, b') = f(b'), \qquad b' \in B',$$
$$\bar{h}(0, g') = \bar{f}(g'), \qquad g' \in G',$$
$$p\bar{h} = Hp' \mid G'.$$

Then h can be extended to $\bar{H}: I \times E' \to E$ such that

$$\bar{H}(0, e') = fe', \qquad p\bar{H} = H(1 \times p').$$

This can be "translated" into the prism language and then proved, using 3.1 and a familiar argument.

By a classical argument (cf. [4], p. 54), we deduce

3.3. Lifting homoptopy extension theorem. *Let (E, B, p) be a fibre-map, $A' \subset B'$ complexes and*

$$f\colon B' \to E, \qquad H\colon I \times B' \to B, \qquad F_A\colon I \times A' \to E$$

maps such that

$$pf(b') = H(0, b'), \qquad pF_A = H \mid I \times A',$$
$$F_A(0, a') = f(a') \qquad\qquad (a' \in A', b' \in B').$$

Then F_A has an extension $F\colon I \times B' \to E$ such that $F(0, b') = f(b')$ and $pF = H$.

4. Retraction on a minimal fibre-map. (cf. [1]).

4.1. THEOREM. *Let (E, B, p) be a fibre-map; there exists a subcomplex $E' \subset E$ such that (E', B, p'), where $p' = p \mid E'$, is a minimal fibre-map and a strong deformation retract of (E, B, p).*

4.2. THEOREM. *Let (E, B, p) be a fibre-map and $B^* \subset B$ a given minimal deformation retract of B; there exists $E^* \subset E$ such that (E^*, B^*, p^*), where $p^* = p \mid E^*$, is minimal and a deformation retract of (E, B, p), the deformation retraction lying over the given one.*

Outline of the proof of 4.1. We call $e, e' \in E_n$ *p-compatible* if $pe = pe'$, $\partial_i e = \partial_i e'$ for $0 \leqq i \leqq n$. p-compatible elements e, e' are said to be *p-homotopic* if there is an element $u \in E_{1.n}$ such that

$$pu = \sigma_1 pe = \sigma_1 pe',$$
$$\lambda^0{}_1 u = e, \qquad \lambda^1{}_1 u = e',$$
$$\partial_i u = \sigma_1 \partial_i e = \sigma_1 \partial_i e'$$

If p is a fibre-map, p-homotopy is an equivalence-relation; degenerate p-homotopic elements are equal; and, most important, p is minimal if and only if p-compatible and p-homotopic elements are equal.

The proof of 4.1 consists in building up E' dimension by dimension always choosing one element only in each p-homotopy class; elements having boundary not already in E' we first "move" into ones that have, using the inductively defined retraction on the boundaries.

The proof of Theorem 4.2 uses a succession of homotopy-covering arguments.

It will appear from 5.2 below that the minimal map obtained in Theorem 4.1 is unique up to an "equivalence."

5. Homotopy and minimal fibre spaces. In view of the last section we can, for the purposes of homotopy-theory, replace any fibre-map by a minimal one; this procedure is useful largely because of the theorems of the present section.

A map $f\colon A \to B$ will be called an *injection* if $fa = fa'$ implies $a = a'$; an injection onto will be called an *equivalence*.

5.1. PROPOSITION. *Let $(\bar{f}_0, f_0), (\bar{f}_1, f_1)\colon (E', B', p') \to (E, B, p)$ be homotopic maps, and let p be a minimal fibre map.*

(i) *If $\bar{f}_0$, f_1 are injective, so is $\bar{f}_1$.*

(ii) *Let $E^\epsilon = p^{-1}(f_\epsilon B')$ $(\epsilon = 0, 1)$. If $\bar{f}_0$, f_0, f_1 are injections onto E^0, f_0E', f_1B' respectively, then $\bar{f}_1$ is an injection onto E^1.*

Proof. We are given homotopies $\bar{H}\colon E' \to E$, $H\colon B' \to B$ such that $p\bar{H} = Hp'$ and $\lambda^0{}_1\bar{H} = \bar{f}_0$, $\lambda^1{}_1H = \bar{f}_1$, $\lambda^0{}_1H = f_0$, $\lambda^1{}_1H = f_1$.

(i) Let $e', e'' \in E'_n$ be such that $\bar{f}_1e' = \bar{f}_1e''$. Then $p\bar{f}_1e' = p\bar{f}_1e''$, i.e. $f_1p'e' = f_1p'e''$, whence $p'e' = p'e'' = b'$ say. Let $w' = \bar{H}e'$, $w'' = \bar{H}e''$. Then $pw' = pw'' = Hb'$, $\lambda^1{}_1w' = f_1e' = f_1e'' = \lambda^1{}_1w''$. If $n = 0$, minimality implies $\lambda^0{}_1w' = \lambda^0{}_1w''$, i.e., $\bar{f}_0e' = \bar{f}_0e''$ and $e' = e''$. If $n > 0$, we use an induction on n and thus have $\partial_ie' = \partial_ie''$ for $0 \leqq i \leqq n$; hence $\partial_iw' = \partial_iw''$, and the same conclusion can be made.

(ii) $\bar{f}_1$ is injective, by (i). Let $e \in E^1{}_n$, $b = pe$. Then there is $b' \in B'$ such that $f_1b' = b$, i.e. $b = \lambda^1{}_1Hb'$.

Hence, if $n = 0$, there is $w \in E_{1,0}$ such that $pw = Hb'$, $\lambda^1{}_1w = e$. Then $\lambda^0{}_1w \in E^0$ and there is $e' \in E'$ such that $f_0e' = \lambda^0{}_1w$. Then

$$f_0p'e' = p\bar{f}_0e' = p\lambda^0{}_1w = \lambda^0{}_1pw = \lambda^0{}_1Hb' = f_0b',$$

whence $p'e' = b'$. Now:

$$p\bar{H}e' = Hp'e' = Hb' = pw,$$
$$\lambda^0{}_1\bar{H}e' = \bar{f}_0e' = \lambda^0{}_1w.$$

Hence $\lambda^1{}_1He' = f_0e' = \lambda^0{}_1w$, by the condition of minimality, i.e. $\bar{f}_1e' = e$, and $\bar{f}_1$ is onto $E^1{}_0$.

For $n > 0$, we use an induction on n; we write down suitable conditions for $\partial_i w$; and in this we require that $\bar{f}_1$ should be injective. We omit the details.

5.2. COROLLARY. *A strong homotopy equivalence between minimal fibre-maps is a strong equivalence. A homotopy equivalence between minimal fibre-maps with minimal base-spaces is an equivalence.*

5.3. *Definition.* Let (E, B, p) and (A, B, f) be maps; we define the map (E^*, A, p^*) and the map $(\bar{f}, f) : (E^*, A, p^*) \to (E, B, p)$ as follows:

$$E^* = \{(e, a) \in E \times A \mid fa = pe\},$$

$$p^*(e, a) = a, \qquad \bar{f}(e, a) = e.$$

(E^*, A, p^*) is called the *map induced from* (E, B, p) *by* $f : A \to B$; the entire assembly of maps and spaces in $(\bar{f}, f)$ is called the *induced structure*

5.4. LEMMA. *If (E, B, p) is a (minimal) fibre-map, so is any map induced from it.*

5.5. PROPOSITION. *Let (E, B, p) be a minimal fibre-map and f_0, f_1: $A \to B$ homotopic maps. Then the induced maps (E^0, A, p^0), (E^1, A, p^1) are strongly equivalent*

Proof. Let $F : I \times A \to B$ be the given homotopy and $(E^*, I \times A, p^*)$ the minimal fibre space induced by F. $p^{*-1}(\epsilon \times A)$ $(\epsilon = 0, 1)$ can be indentified with E^ϵ. Now, consider the commutative diagram

$$\begin{tikzcd} I \times E^0 \arrow[r, "\phi"] \arrow[d, "1 \times p^0"'] & E^* \arrow[d, "p^*"] \\ I \times A \arrow[r, "1"'] & I \times A, \end{tikzcd}$$

where $\phi \mid 0 \times E^0$ is the identity; such a map ϕ exists by 3.2. Now,

$$\phi^0 = \phi \mid 0 \times E^0 \qquad (= 1),$$
$$\phi^1 = \phi \mid 1 \times E^0$$

can be regarded in a natural manner as maps $E^0 \to E^*$; they satisfy the conditions on f_0, f_1 in 5.1 (ii). Hence ϕ^1 is an isomorphism $E^0 \to E^1$.

5.6. COROLLARY. *A minimal fibre space with a contractible base-space is a product space.*

IV. Fibre Bundles.

1. The group complex $A(Y)$. Let X, Y be complexes. By X^Y (cf. [1], [2]) we denote the complex whose n-elements are maps

$$\alpha\colon \Delta^n \times Y \to X,$$

and we define $\partial_i\alpha = \alpha(\epsilon^i \times 1)$, $s_i\alpha = \alpha(\eta^i \times 1)$ (cf. II.1). Sometimes it is convenient to replace α by the map $\alpha_I\colon \Delta^n \times Y \to \Delta^n \times X$ given by $\alpha_I(t,y) = (t, \alpha(t,y))$, $t \in \Delta^n$, $y \in Y$. Clearly α and α_I determine each other.

Let X, Y, Z be complexes, and let $\alpha \in X^Y$, $\beta \in Y^Z$; we define $\alpha\beta \in X^Z$ by $(\alpha\beta)_I = \alpha_I\beta_I$. It is easily verified that

$$\partial_i(\alpha\beta) = (\partial_i\alpha)(\partial_i\beta), \qquad s_i(\alpha\beta) = (s_i\alpha)(s_i\beta).$$

The complex Y^Y is a monoid under this operation; it operates on Y according to

$$\alpha \cdot y = \alpha(\delta^n, y), \qquad \alpha \in (Y^Y)_n, \qquad y \in Y_n.$$

We define $A(Y) \subset Y^Y$ to be the maximal subgroup; thus $\alpha \in Y^Y$ is in $A(Y)$ if and only if α_I has an inverse. $A(Y)$ is a group-complex and hence (cf. [1]) a Kan-complex.

$A(Y)$ has an important universal property: Let Γ be any group-complex operating on Y; we define the homomorphism

$$\rho\colon \Gamma \to A(Y)$$

by $(\rho\gamma)(\phi\delta^n, y) = (\phi\gamma)y$, where $\gamma \in \Gamma$, $y \in Y$ and ϕ is a suitable semisimplicial operator. Then $\gamma y = (\rho\gamma) \cdot y$. If Γ is effective, i.e., if ρ is a monomorphism, we shall thus regard Γ as a subgroup of $A(Y)$, identifying y and ρy; replacing (where necessary) Γ by $\Gamma/\mathrm{kernel}\,\rho$, *we restrict ourselves to this case from now on.*

2. Fibre bundles.

2.1. *Definition.* The map (E, B, p) will be called a *fibre-bundle* if

(i) p is onto.

(ii) For every map $b\colon \Delta^n \to B$ the induced map (E^b, Δ^n, p^b) is strongly equivalent to $(\Delta^n \times Y, \Delta^n, p^*)$, where $p^*(\phi\delta^n, y) = \phi\delta^n$ and Y is a given complex called the *fibre* of the bundle.

If Y is a Kan-complex, we call (E, B, p) a *Kan fibre-bundle.*

From III. 5. 6 we have immediately

2.2. PROPOSITION. *Every minimal fibre map with a connected base complex is a Kan fibre bundle.*

The following is easy:

2.3. PROPOSITION. *Every Kan fibre bundle is a fibre map.*

Let (E, B, p) be a fibre-bundle with fibre Y; regarding $b \in B_n$ as a map $b: \Delta^n \to B$ (cf. II.1) we have the commutative diagram

$$\begin{tikzcd} \Delta^n \times Y \arrow[r, "\alpha(b)"] \arrow[d, "p^*"] & E^b \arrow[r, "\bar{b}"] \arrow[d, "p^b"] & E \arrow[d, "p"] \\ \Delta^n \arrow[r, "1"'] & \Delta^n \arrow[r, "b"'] & B, \end{tikzcd}$$

where $\alpha(b)$ is an equivalence exhibiting the strong equivalence of 2.1(ii). The set of equivalences $\{\alpha(b)\}$ for $b \in B$ is called an *atlas* for the bundle. We also define

$$\beta(b) = \bar{b}\alpha(b).$$

Observe that $\alpha(b)(\phi\delta^n, y) = (\phi\delta^n, \beta(b)(\phi\delta^n, y))$ so that the atlas $\{\alpha(b)\}$ and the set of maps $\{\beta(b)\}$ determine each other.

The choice of an atlas is highly arbitrary; if $\{\alpha(b)\}$, $\{\bar{\alpha}(b)\}$ are two atlases, then

$$(\alpha(b))^{-1}\bar{\alpha}(b) = \gamma_I(b)$$

is an element of $A(Y)_n$. Conversely, if for every $b \in B_n$ we choose $\gamma(b) \in A(Y)_{n-1}$ and if $\{\alpha(b)\}$ is a given atlas, then $\{\bar{\alpha}(b)\}$ given by

$$\bar{\alpha}(b) = \alpha(b)\gamma_I(b) \tag{1}$$

is another. Notice that also

$$\bar{\beta}(b) = \beta(b)\gamma(b). \tag{2}$$

Given an atlas $\{\alpha(b)\}$, $\beta(b) \in E^Y$ for every $b \in B$. In general it is not true that

$$\beta(s_i b) = s_i \beta(b). \tag{3}$$

By the simple device, however, of defining $\beta(b)$, and hence $\alpha(b)$, on all degenerate elements by (3) above we can always replace an atlas by a *normalised atlas*, i.e., one for which (3) above is true. From now on we shall invariably suppose atlases to be normalised.

More interesting considerations arise from the face operators. Let $b \in B_n$. $\alpha(b)$ maps $\Delta^{n-1} \times Y$ isomorphically onto the part of E^b "over" $\delta_i\delta^n$; hence there is an isomorphism $\alpha_i(b) : \Delta^{n-1} \times Y \to E^{\delta_i b}$ such that the diagram

$$\begin{tikzcd}
\Delta^n \times Y \arrow[r, "\alpha(b)"] & E^b \arrow[r, "\tilde{b}"] & E \\
\Delta^{n-1} \times Y \arrow[u, "\epsilon^i \times 1"'] \arrow[r, "\alpha_i(b)"'] & E^{\partial_i b} \arrow[u, "\bar{\epsilon}^i \times 1"'] \arrow[r, "\widetilde{\partial_i b}"'] & E \arrow[u, "1"']
\end{tikzcd}$$

commutes $(0 \leqq i \leqq n)$. The important thing is that, in general, $\alpha_i(b) \neq \alpha(\partial_i b)$, i.e., $\partial_i\beta(b) \neq \beta(\partial_i b)$. We define

$$(4) \qquad \xi^i{}_I(b) = [\alpha(\partial_i b)]^{-1}\alpha_i(b) \in A(Y)_{n-1}$$

and refer to $\{\xi^i(b)\}$ as the set of *transformation elements* associated with the atlas $\{\alpha(b)\}$.

From (4) we get immediately

$$(5) \qquad \alpha_i(b) = \alpha(\partial_i b)\xi^i{}_I(b),$$

whence

$$(6) \qquad \partial_i\beta(b) = \beta(\partial_i b)\xi^i(b).$$

2.4. *Definitions.* Let $\Gamma \subset A(Y)$ be a subgroup-complex. An atlas $\{\alpha(b)\}$ all of whose transformation-elements lie in Γ will be called a Γ-*atlas*; two Γ-atlases $\{\alpha(b)\}$, $\{\bar{\alpha}(b)\}$ will be called Γ-*equivalent* if $\bar{\alpha}(b) = \alpha(b)\gamma_I(b)$, where $\gamma(b) \in \Gamma$. A fibre-bundle together with a given Γ-equivalence-class of Γ-atlases will be called a Γ-*bundle*; thus any bundle with fibre Y is an $A(Y)$-bundle.

Let (E, B, p), $(\bar{E}, \bar{B}, p)$ be Γ-bundles; a map $(f, g) : (E, B) \to (\bar{E}, \bar{B})$ will be called a Γ-*map* if for every $b \in B$

$$[\bar{\alpha}(fb)]^{-1} \circ f \circ \alpha(b)$$

is an element of Γ, provided that $\{\alpha(b)\}$ and $\{\bar{\alpha}(\bar{b})\}$ belong to the given Γ-equivalence classes of atlasses; notice the consequential notions of "Γ-equivalence" and "strong Γ-equivalence"; for bundles with fibre Y, "equivalence" and "$A(Y)$-equivalence" are the same notions.

From now on we will formulate everything for the general case of Γ-bundles.

Let $\Lambda \subset \Gamma$ be a subgroup-complex; if in the given Γ-equivalence-class of atlases of a given Γ-bundle there is a Γ-bundle there is a Λ-atlas, we say that

the *group of the bundle can be reduced to* Λ; notice, however, that the resulting Λ-bundle will, in general, not be unique.

2.5. LEMMA. *In every* Γ-*equivalence class of atlases there is one for which* $\xi^i(b)=1$ *for* $i>0$.

Proof. Let $b\in B_n$. If $n=1$, since Γ (being a group-complex) is a Kan-complex we can find $\gamma\in\Gamma_1$ such that $\partial_1\gamma=\xi^1(b)$. We replace $\alpha(b)$ by $\bar\alpha(b)=\alpha(b)\gamma^{-1}{}_I$. Then $\partial_1\beta(b)=\beta(\partial_1 b)\xi^1(b)[\xi^1(b)]^{-1}=\beta(\partial_1 b)$.

Now suppose inductively that $\{\alpha(b)\}$ satisfies the lemma up to dimension $n-1$, $n\geqq 2$, and let $b\in B_n$ be non-degenerate. From the inductive hypothesis it is easy to verify $\partial_i\xi^j(b)=\partial_{j-1}\xi^i(b)$ if $0<i<j$. Hence there is $\gamma\in\Gamma_n$ such that $\partial_i\gamma=\xi^i(b)$ for $i<0$. We replace $\alpha(b)$ by $\bar\alpha(b)=\alpha(b)\gamma^{-1}{}_I$. Then, for $i>0$, $\partial_i\bar\beta(b)=\beta(\partial_i b)\xi^i(b)[\xi^i(b)]^{-1}=\beta(\partial_i b)$.

2.6. LEMMA. *Let* $\Lambda\subset\Gamma$ *be a subcomplex which is a deformation retract of* Γ. *Then in every* Γ-*equivalence class of atlases there is one for which*

$$\xi^i(b)=1, \qquad i>0,$$
$$\xi^0(b)\in\Lambda.$$

Proof. Let $N:\Gamma\to\Gamma$ be the given retracting homotopy, so that $\lambda^0{}_1U=1$, $\lambda^1{}_1U\gamma\in\Lambda$, $U\mid\Lambda=\sigma_1$. Let the given atlas $\{\alpha(b)\}$ already satisfy the conditions of 2.5 and, inductively, $\xi^0(b)\in\Lambda$ if $\dim b<n$. Now let $b\in B_n$ and $\xi=\xi^0(b)$. Then it is easily verified that $\partial_i\xi\in\Lambda$ for all i. By the Kan-condition (and cf. [2]) there is a prism $T\in\Gamma_{1,n}$ such that

$$\lambda^0{}_1T=s_0\xi,\qquad \partial_iT=\sigma_1\partial_is_0\xi \qquad (i>0),$$
$$\partial_0T=U\xi,$$

since these faces are consistent. Now, let $\gamma=(s_0\xi)^{-1}(\lambda^1{}_1T)$. Then, as is easily verified,

$$\partial_i\gamma=1 \qquad (i>0),$$
$$\partial_0\gamma=\xi^{-1}\lambda,$$

where $\lambda=\lambda^1{}_1U\xi\in\Lambda$.

Now, replace $\alpha(b)$ by $\bar\alpha(b)=\alpha(b)\gamma_I$, so that $\bar\beta(b)=\beta(b)\gamma$. Then $\partial_i\bar\beta(b)=\beta(\partial_ib)$, $i>0$, and $\partial_0\bar\beta(b)=\beta(\partial_0b)\xi\xi^{-1}\lambda=\beta(\partial_0b)\lambda$.

3. Twisted Cartesian products.

3.1. *Definition.* Let B, Y be complexes. A *twisted cartesian product*

(TCP) $B \tilde{\times} Y$ is a complex for which $(B \tilde{\times} Y)_n = B_n \times Y_n$ $(n \geqq 0)$ and

$$\partial_i(b,y) = (\partial_i b, \partial_i y) \qquad (0 < i \leqq n, n > 0),$$
$$\partial_0(b,y) = (\partial_0 b, \tau(b,y)), \qquad b \in B_n, y \in Y_n,$$

where $\tau(b,y) \in Y_{n-1}$.

τ is called the *twisting function.*

From the semisimplicial identities the following identities follow for τ:

$$(1) \qquad \begin{aligned} \tau(\partial_1 b, \partial_1 y) &= \tau(\partial_0 b, \tau(b,y)), \\ \partial_i \tau(b,y) &= \tau(\partial_{i+1} b, \partial_{i+1} y), \qquad i > 0, \\ s_i \tau(b,y) &= \tau(s_{i+1} b, s_{i+1} y), \\ \tau(s_0 b, s_0 y) &= y. \end{aligned}$$

The twisted cartesian product (and τ) are called *semi-regular* if $\tau(b,y)$ depends on b and $\partial_0 y$ only.

We refer to a *regular* TCP (RTCP) if for every $b \in B_n$ $(n > 0)$, there is an element $\xi(b) \in A(Y)_{n-1}$ such that

$$\tau(b,y) = \xi(b) \cdot \partial_0 y.$$

If for every $b \in B$, $\xi(b)$ lies in a subgroupcomplex Γ of $A(Y)$ the RCTP is said to *have group* Γ.

By virtue of (1), the function ξ must satisfy the following identities

$$(2) \qquad \begin{aligned} \partial_0 \xi(b) &= [\xi(\partial_0 b)]^{-1} \xi(\partial_1 b), \\ \partial_i \xi(b) &= \xi(\partial_{i+1} b), \qquad i > 0, \\ s_i \xi(b) &= \xi(s_{i+1} b), \qquad i \geqq 0, \\ \xi(s_0 b) &= 1. \end{aligned}$$

Let $E = B \tilde{\times} Y$; we define the map $p: E \to B$ by $p(b,y) = b$; from now on, with a slight abuse of language, the term "TCP" will also stand for the map $(B \tilde{\times} Y, B, p)$.

3.2. PROPOSITION. *A fibre bundle whose group can be reduced to* Γ *is* (*strongly equivalent to*) *a* RTCP *with group* Γ.

Proof. Let (E, B, p) be a fibre bundle with fibre y and group Γ, and let $\{\alpha(b)\}$ be a Γ-atlas satisfying the conditions of 2.5 above, we define

$$\xi(b) = \xi^0(b), \qquad b \in B_n, n \geqq 1$$

and the functions

$$h: B_n \times Y_n \to E_n$$

by

$$h(b,y) = \beta(b)(\delta^n, y).$$

Then the following are easily verified:

(i) h is $1-1$ and onto; it is easy to write down an inverse;

(ii)
$$\partial_i h(b,y) = h(\partial_i b, \partial_i y) \qquad (i > 0), \qquad \text{and}$$
$$\partial_0 h(b,y) = h(\partial_0 b, \xi(b)\cdot\partial_0 y); \text{ as well as}$$
$$s_i h(b,y) = h(s_i b, s_i y).$$

Notice that once the atlas is given, h is determined without further choice; thus, if we define a Γ-map between two RTCP $B\widetilde{\times}Y$, $B'\widetilde{\times}Y$, both with group Γ, as one having the form $(b,y)\to(gb,\theta(b)\cdot y)$, where $g: B\to B'$ is a map and $\theta: B\to\Gamma$ a certain function; then the corresponding notion of a Γ-equivalence class of RTCP corresponds, under the function h, exactly to that of a Γ-equivalence class of Γ-bundles, cf. 2.4 above. We omit the easy verifications.

3.3. PROPOSITION. *An* RTCP *whose fibre is a Kan-complex is a Kan fibre-space.*

The verification is easy.

4. Principal and associated bundles. Let Γ be a group complex; in what follows we shall always suppose that Γ operates on itself from the left by multiplication; this leads to a natural embedding $\Gamma\subset A(\Gamma)$.

4.1. *Definition.* A Γ-bundle with fibre Γ is called a *principal Γ-bundle.*

If (E,B,p) is a principal Γ-bundle, it is possible to define an operation of Γ on the *right* of E satisfying $p(e\gamma)=p(e)$, as follows:

Let $\{\alpha(b)\}$ be a Γ-atlas in the Γ-equivalence-class of atlases defining the given Γ-bundle, let $e\in E$, $pe=b$, and

$$e=\beta(b)(\delta^n,\gamma).$$

Then we define

$$e\gamma'=\beta(b)(\delta^n,\gamma\gamma').$$

It is easily verified that this *does* define an operation which is independent

If we express a principal Γ-bundle as a RCTP, then $\xi(b) \in \Gamma$, and the operation of Γ takes the simple form

$$(b, \gamma)\gamma' = (b, \gamma\gamma').$$

Let Γ operate on the right of the complex E and on the left of the complex Y; we define $E \times_\Gamma Y$ by identifying $(e\gamma, y)$ and $(e, \gamma y)$ in $E \times Y$.

4.2. *Definition.* Let (E, B, p) be a given principal Γ-bundle and Y a complex on which Γ operates; we define the *associated bundle* (E^*, B, p^*) by

$$E^* = E \times_\Gamma Y, \qquad p^*(e, y) = pe.$$

It is easily verified that (E^*, B, p^*) is a bundle with fibre Y; indeed, let $\{\alpha(b)\}$ be an atlas for (E, B, p); then we define the atlas $\{\alpha^*(b)\}$ for (E^*, B, p^*) by

$$\beta^*(b)(\phi\delta^n, y) = (\beta(b)(\phi\delta^n, 1), y).$$

In this way we see that

4.3. Proposition. *For a given principal Γ-bundle and a given complex Y on which Γ operates on the left, there is a unique associated Γ-bundle with fibre Y.*

4.4. Proposition. *Every Γ-bundle with fibre Y is associated to a principal Γ-bundle which is uniquely determined.*

Proof. We take the Γ-bundle in the form of a RCTP with twisting function $\xi(b)$; the principal RTCP with the same twisting function is the required principal Γ-bundle; the fact that any RTCP *is* a fibre bundle is proved in 5.3 below.

5. Classification theorems. Let us use the notation of III. 5.5 for the structure induced from the map (E, B, p) by the map $f\colon A \to B$.

According as (E, B, p) *is* a fibre-bundle, Γ-bundle or principal bundle, so is (E^*, A, p^*); in particular the atlases are related by

$$\bar{f}\beta^*(a) = \beta(fa);$$

it is in this way that a Γ-equivalence-class of atlases for (E, B, p) determines one for (E^*, A, p^*); in the case of principal bundles we have

$$\bar{f}(e^*\gamma) = [\bar{f}(e^*)]\gamma,$$

i.e. $\bar{f}$ is equivariant.

If E is a RTCP, $E = B \tilde{\times} Y$, then so is E^*; the twisting function is given by

$$\xi^*(a) = \xi({}^{*}_{1}a).$$

Now, let (E, B, p) be a principal Γ-bundle and $U : A \to B$ a homotopy; we write $\lambda^i{}_1 U = f_i$; $(i = 0, 1)$, and denote by

$$(\bar{f}_i, f_i) : (E_i, A, p_i) \to (E, B, p)$$

the induced structures.

For the next lemma notice that if a multiplication is defined amongst elements of complexes, then this implies one between prisms.

5.1. Lemma. *There exists a homotopy*

$$V : E_0 \to E$$

such that

$$pV = Up_0,$$
$$\lambda^0{}_1 V = \bar{f}_0,$$
$$V(e_0\gamma) = (Ve_0)(\sigma_1\gamma) \qquad (e_0 \in E_0, \gamma \in \Gamma).$$

Proof. This is proved exactly like III. 3. 2, except having "lifted" V to some chosen $e_0 \in p_0^{-1}(b)$, we define it on the rest of $p_0^{-1}(b)$ by equivalence, i.e., by $V(e_0\gamma) = (Ve_0)(\sigma_1\gamma)$; this is possible since $p_0^{-1}(b) = e_0\Gamma$, as is evident.

Now, let us suppose that (E, B, p) is expressed as a RSTP $B \tilde{\times} \Gamma$ with twisting function ξ. Then

$$\lambda^1{}_1 V(a, \gamma) = (f_1 a, \theta(a)\gamma),$$

where $\theta(a)$ is defined by $(\lambda^1{}_1 V)(a, 1) = (f_1 a, \theta(a))$. The function $\theta : A \to \Gamma$ satisfies certain identities.

5.2. Proposition. *Homotopic maps induce Γ-equivalent bundles from a given Γ-bundle.*

Proof. Take the given Γ-bundle in the form of a RTCP $B \times Y$ with twisting function ξ. Let $U : A \to B$ be the given homotopy, and construct $\theta : A \to \Gamma$ as above. Then

$$(a, y) \to (a, \theta(a) \cdot y)$$

gives the equivalence. Several verifications are left to the reader.

Notice that the proof only uses the fact that we have a RTCP: hence we see that any RTCP which has a contractible base-space is a product space; in particular

5.3. PROPOSITION. *Any* RTCP *is a fibre-bundle.*

Remark. A semi-regular TCP is a fibre-bundle provided it is a Kan fibre-map; we omit the somewhat complicated proof.

For any group-complex Γ, the well-known "W-construction" provides a classifying space $\bar{W}(\Gamma)$; we recall briefly the definition, which we modify by inverting the usual order of elements; this is done to assure operation on the right.

Given Γ, we define the RTCP $(W(\Gamma), \bar{W}(\Gamma), p)$ as follows:

$$W_0(\Gamma) = \Gamma_0,$$
$$W_{q+1}(\Gamma) = W_q(\Gamma) \times \Gamma_{q+1},$$

and Γ_q acts on $W_q(\Gamma)$ by the definition

$$(\gamma_0, \gamma_1, \cdots, \gamma_q) \cdot \gamma'_q = (\gamma_0, \gamma_1, \cdots, \gamma_{q-1}, \gamma_q \cdot \gamma'_q), \quad \text{where } \gamma_i \in \Gamma_i,\ \gamma'_q \in \Gamma_q.$$

The semisimplicial operators are defined as follows: s_0 on $W_0(\Gamma) = s_0$ on Γ_0. Now, let $w \in W_q(\Gamma)$ and $\gamma \in \Gamma_{q+1}$, so that $(w, \gamma) \in W_{q+1}(\Gamma)$; then we define inductively

$$\partial_0(w, \gamma) = w \cdot \partial_0\gamma,$$
$$\partial_{i+1}(w, \gamma) = (\partial_i w, \partial_{i+1}\gamma),$$
$$s_0(w, \gamma) = (w, 1, s_0\gamma),$$
$$s_{i+1}(w, \gamma) = (s_i w, s_{i+1}\gamma).$$

Next, we define $\bar{W}(\Gamma)$ as follows:

$$\bar{W}_0(\Gamma) \text{ consists of a single element denoted by } [\ ],$$
$$\bar{W}_{q+1}(\Gamma) = \bar{W}_q \times \Gamma_q.$$

Thus, if $w \in W_q(\Gamma)$, we denote by $[w]$ the corresponding element of $\bar{W}_{q+1}(\Gamma)$.

We define $p\colon W(\Gamma) \to \bar{W}(\Gamma)$ by $p(w, \gamma) = [w]$, $p\gamma = [\ ]$ if $\gamma \in \Gamma_0$. Suitable semisimplicial operators in $\bar{W}(\Gamma)$ are now easily written down; it turns out that $W(\Gamma) = \bar{W}(\Gamma) \tilde{\times} \Gamma$ is a principal RTCP with twisting function

$$\xi[\gamma_0, \gamma_1, \cdots, \gamma_{q-1}] = \gamma_{q-1}.$$

Now, let $E = B \widetilde{\times} \Gamma$ be a principal RTCP with twisting function ξ. We define the map

$$k_\xi \colon B \to \bar{W}(\Gamma)$$

by

$$k_\xi(b) = [\xi(\partial^{n-1}{}_0 b), \xi(\partial^{n-2}{}_0 b), \cdots, \xi(b)] \quad \text{if} \quad b \in B_n.$$

5.4. Lemma. (i) *k_ξ is a map.*

(ii) *k_ξ induces the given* RTCP *from* $(W(\Gamma), \bar{W}(\Gamma), p)$.

The verifications are straightforward.

5.5. Proposition. *The assignment $\xi \to k_\xi$ set up a* 1-1 *relationship between homotopy-classes of maps $B \to \bar{W}(\Gamma)$ and strong Γ-equivalence-classes of principal Γ-bundles with base-complex B.*

Proof. Homotopic maps induce equivalent bundles, by 5.3. It remains to prove the converse. Thus, let $k_0, k_1 \colon B \to \bar{W}(\Gamma)$ be maps with induced structures $(\tilde{k}_\epsilon, k_\epsilon) \colon (E_\epsilon, B, p_\epsilon) \to (W(\Gamma), \bar{W}(\Gamma), p)$, $\epsilon = 0, 1$; and suppose there is a strong Γ-equivalence $(\tilde{k}, 1) \colon (E_0, B, p_0) \to (E_1, B, p_1)$.

Consider the maps $\tilde{k}_0, \tilde{k}_1\tilde{k} \colon E \to W(\Gamma)$. We shall construct an equivariant homotopy connecting them; i.e., a homotopy

$$V \colon E_0 \to W(\Gamma)$$

such that $\lambda^0{}_1 V = \tilde{k}_0$, $\lambda^1{}_1 V = \tilde{k}_1\tilde{k}$,

$$V(e_0\gamma) = (V(e_0))\sigma_1\gamma.$$

Suppose, inductively, V has been defined up to dimension $n-1$ and let $e_0 \in (E_0)_n$ be some chosen element. An element $V(e_0)$ satisfying the conditions exists because $W(\Gamma)$ has trivial homotopy-groups; we define $V(e_0\gamma)$ by the condition of equivariance.

Now, we define a homotopy $U \colon B \to \bar{W}(\Gamma)$ by choosing for each $b \in E_n$ an $e_0 \in (E_0)_n$ such that $p_0 e_0 = b$; and take $U(b) = pV(e_0)$; due to the condition of equivariance on V, U is well-defined. Now,

$$\lambda^0{}_1 U(b) = p\tilde{k}_0(e_0) = k_0 p_0 e_0 = k_0 b,$$

$$\lambda^1{}_1 U(b) = p\tilde{k}_1\tilde{k}(e_0) = k_1 p_1 \tilde{k} e_0 = k_1 p_0 b_0 = k_1 b,$$

and thus U is the required homotopy.

5.6. Theorem. *Let Y be a complex on which the group complex Γ operates effectively. The assignment to any map $B \to \bar{W}(\Gamma)$ of the bundle*

with fibre Y associated to the principal Γ-bundle over B induced from $(W(\Gamma), \bar{W}(\Gamma), p)$ is a 1-1 correspondence between homotopy-classes of maps $B \to \bar{W}(\Gamma)$ and strong Γ-equivalence-classes of Γ-bundles with base B and fibre Y.

Notice, in particular, the special case obtained by putting $\Gamma = A(Y)$, and replacing "Γ-bundle" by "bundle" "Γ-equivalence" by "equivalence."

REFERENCES.

[1] J. C. Moore, *Lectures on Homotopy theory* (1955-56, Princeton, Mimeographed).

[2] V. K. A. M. Gugenheim, "On supercomplexes," *Transactions of the American Mathematical Society*, vol. 85 (1957), p. 35.

[3] ——— and J. C. Moore, "Acyclic models and fibre spaces," *ibid.*, vol. 85 (1957), p. 265.

[4] N. E. Steenrod, *The topology of fibre bundles*, Princeton, 1951.

SINGULAR INTEGRALS ON COMPACT MANIFOLDS.*

By R. T. SEELEY.[1]

TABLE OF CONTENTS

Introduction. Singular integrals have been studied intermittently for over twenty years, on both Euclidean space and on manifolds, primarily by Giraud, Tricomi, Mihlin, Calderon and Zygmund, and Kohn. The work of the first three authors is summarized in [6]. Calderon and Zygmund have

* Received November 24, 1958.

[1] Part of the research for this paper was done while the author was assisted by National Science Foundation Grant G2265.

considered these operators on the spaces $L^p(E_k)$, $(1 < p < \infty)$, E_k being k-dimensional Euclidean space. In this case they have shown that singular integrals define bounded operators [1], that there is an approximate functional calculus for such operators resembling the Fourier transform apparatus [2], and that they may be used to represent differential operators [2]. This representation has been used in solving uniqueness problems [3] and is likely to have further applications in differential equations.

The present paper obtains for compact manifolds results like those in [2]. Kohn, in a paper with Spencer [5], has considered similar problems but is concerned mainly with the question of regularization, and the fitting of singular integral operators into the formalism of differential geometry. Here the two main objectives are the formulation of the notion of a singular integral operator on a compact manifold, and the development of an approximate functional calculus (section II); and the construction of an isotropic first order differential operator on a compact, orientable Riemannian manifold M allowing the representation of differential operators on $L^p(M)$ (section III). Section I establishes the notation and contains the Euclidean results used in the later sections, as well as a few related results. In the construction in section III, singular integral operators are used to establish some facts about the Laplace operator on $L^2(M)$ previously given by Gaffney [4].

The results labeled "proposition" are those that are easily accessible with the tools developed, but do not form part of the main argument.

This paper is a revision of the author's thesis of the same title submitted to MIT in 1958. Naturally it owes much to the supervisor, Professor Calderon, who suggested the general topic, the consideration of the distribution spaces, the present formulation of section II without a metric (considerably neater than the original form), and that the operators needed in section III might be constructed by contour integration; and whose comments on earlier versions led to much improvement in the presentation. The author, on the other hand, is responsible for the actual proofs.

I. Miscellaneous Euclidean Results

A. Notation and preliminary definitions. Let E_k be k-dimensional Euclidean space and $\alpha = (\alpha_1, \cdots, \alpha_k)$ a k-tuple of non-negative integers. If $x = (x_1, \cdots, x_k)$ is a point in E_k, then $x^\alpha = \prod_{i=1}^{k} x_i^{\alpha_i}$. Let $|\alpha| = \sum_i \alpha_i$ and $\alpha! = \prod_i (\alpha_i!)$. Then $(\partial/\partial x)^\alpha = \prod_i (\partial/\partial x_i)^{\alpha_i} = \partial^{|\alpha|}/\partial x_1^{\alpha_1} \cdots \partial x_k^{\alpha_k}$. $f^{(\alpha)}(x)$

denotes $(\partial/\partial x)^\alpha f(x)$; so $(1/\alpha!)(x^\alpha)^{(\beta)}$ is $x^{\alpha-\beta}/(\alpha-\beta)!$ if $\alpha_i \geqq \beta_i$ for all i $(\alpha \geqq \beta)$, and is 0 otherwise. The Taylor expansion becomes

$$f(y) = \sum_{0 \leqq |\alpha| \leqq n} (1/\alpha!) f^{(\alpha)}(x)(y-x)^\alpha + R(x,y).$$

Here the remainder can be differentiated with respect to y as often as f can. The rule for differentiating products takes the form

$$(fg)^{(\alpha)} = \sum_{\alpha \geqq \gamma} f^{(\gamma)} g^{(\alpha-\gamma)} \alpha! / \{\gamma!(\alpha-\gamma)!\}.$$

For a function $f(x,y)$ on $E_k \times E_k$, $f^{(\alpha,\beta)}(x,y)$ denotes $(\partial/\partial x)^\alpha (\partial/\partial y)^\beta f(x,y)$. Differentiation of the Taylor expansion above shows that $R^{(\alpha,\beta)}(x,y)$ is $O(|x-y|^{n+1-|\alpha|-|\beta|})$ if $|\alpha| + |\beta| \leqq n+1$.

If h is a complex function, h^* is its conjugate; if H operates on a Banach space, H^* is its adjoint.

If β is a real number $\geqq 0$, then $[\beta]$ indicates either the greatest integer which is $\leqq \beta$, or a reference to the bibliography. A function f is in C_n if it and its derivatives of order $\leqq n$ are continuous and bounded. A function is in C_β if it and its derivatives of order $\leqq [\beta]$ satisfy a uniform Hölder condition of order $\beta - [\beta]$.

Definition 1. A $C_\beta{}^\infty$ function homogeneous of degree n is a function $h(x,z)$ on $E_k \times E_k$ satisfying:

i) $h(x, \lambda z) = \lambda^n h(x,z)$ for all x, all $z \neq 0$, and all $\lambda > 0$.

ii) For each x, $h(x,z)$ is in C_∞ in $|z| \geqq 1$.

iii) For each α, $(\partial/\partial z)^\alpha h(x,z)$ is in C_β on $E_k \times (|z| \geqq 1)$.

iv) If $n = -k$, $\int_{|z|=1} h(x,z)\, d\sigma = 0$, where $d\sigma$ is the natural measure on $|z| = 1$.

Condition (iv) may seem unnatural, but in this paper we shall always require it of homogeneous functions of degree $-k$. It is justified to some extent by the following fact.

LEMMA 1. *If $h(x,z)$ is a $C_\beta{}^\infty$ function homogeneous of degree n, then $(\partial/\partial z_i) h(x,z)$ is a $C_\beta{}^\infty$ function homogeneous of degree $n-1$.*

Proof. The degree of homogeneity is trivial. The only case that needs checking is $n = 1-k$; then we must show that $h_i(x,z) = (\partial/\partial z_i) h(x,z)$ has mean value zero on $|z| = 1$. Let $\phi(y) = 1$ on $|x-y| \leqq 1$, and vanish outside a compact set. Then

$$\int (\partial\phi(y)/\partial y_i)h(x,x-y)\,dy = \lim_{\epsilon\to 0}\int_{|x-y|=\epsilon}(\partial\phi(y)/\partial y_i)h(x,x-y)\,dy$$
$$=\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}\phi(y)h_i(x,x-y)\,dy - \lim_{\epsilon\to 0}\int_{|x-y|=\epsilon}\phi(y)h(x,x-y)\gamma_i\epsilon^{k-1}\,d\sigma,$$

where $d\sigma$ is the measure on the unit sphere, $y=x+\epsilon\sigma$, and $\gamma_i=(y_i-x_i)/|y-x|$ is the i-th direction cosine. The last limit is $-\int_\Sigma h(x,\sigma)\gamma_i\,d\sigma$, where Σ is the unit sphere. Then $\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}\phi(y)h_i(x,x-y)\,dy$ must exist. But this is

$$\lim_{\epsilon\to 0}\int_{1\geqq|x-y|>\epsilon}h_i(x,x-y)\,dy + \int_{|x-y|>1}\phi(y)h_i(x,x-y)\,dy$$
$$=\lim_{\epsilon\to 0}\int_\Sigma h_i(x,\sigma)\,d\sigma\int_\epsilon^1(1/\rho)\,d\rho + \int_{|x-y|>1}\phi(y)h_i(x,x-y)\,dy.$$

This can have a limit only if the first term is zero, which proves Lemma 1.

Homogeneous $C_\beta{}^\infty$ functions of degree $-k$ are the kernels of the $C_\beta{}^\infty$ singular integral operators studied by Calderon and Zygmund ([1] and [2]). A $C_\beta{}^\infty$ singular integral operator is any of the form

$$Hf(x) = a(x)f(x) + \lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}h(x,x-y)f(y)\,dy,$$

where $h(x,z)$ is a $C_\beta{}^\infty$ function, homogeneous of degree $-k$, and $a(x)$ is in C_β. The limit exists strongly for f in L^p, $1<p<\infty$ [1]. In [2] the above authors develop an approximate functional calculus for such operators, and demonstrate a connection to differential equations.

An important tool in this development is the expansion of h in spherical harmonics. Let $Y_{nm}(z)$ $(|z|=1)$ be a spherical harmonic of degree n, and let the set $\{1, Y_{nm}(z)\}$ form a complete orthonormal basis of L^2 of the unit sphere in E_k. Extend Y_{nm} to $|z|>0$ by setting $Y_{nm}(z)=Y_{nm}(z/|z|)$. Then if $h(x,z)$ is a $C_\beta{}^\infty$ function homogeneous of degree $-k$,

$$h(x,z)=\sum a_{nm}(x)Y_{nm}(z)|z|^{-k}$$

and the a_{nm} and their derivatives of order $\leqq[\beta]$ are $O(n^{-r})$ for every $r>0$. The operators T_{nm} are defined by

$$T_{nm}f(x)=\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}Y_{nm}(x-y)f(y)\,dy,$$

and the operator H is represented by the series $H=a+\sum a_{nm}T_{nm}$. The operators T_{nm} correspond to multiplication of the Fourier transform by a bounded function, so that they commute with differentiation. It is noted that

the number of Y_{nm} for fixed n is $O(n^{k-2})$, and the norm of T_{nm} on L^p has a bound independent of n and m so that the series is norm convergent. (See [2].)

B. The fractional integrals of M. Riesz in connection with singular integrals. In [7], M. Riesz constructs, among other things, a one-parameter group of (unbounded) operators I^α defined for f in C_∞ with compact support in E_k. They satisfy the relations $I^{-2} = -\Delta$, where Δ is the Laplace operator on E_k; and $I^{\alpha+\beta} = I^\alpha I^\beta$ whenever the composition is defined. For $\alpha > 0$, I^α is defined as

$$I^\alpha f(x) = H(\alpha, k)^{-1} \int f(y) \,|\, x - y \,|^{\alpha-k} \, dy,$$

where $H(\alpha, k) = 2^\alpha \pi^{k/2} \Gamma(\alpha/2)/\Gamma(\frac{1}{2}(k-\alpha))$. For $\alpha \leqq 0$, $I^\alpha f(x)$ is defined by analytic continuation with respect to α. Since I^{-1} is a square root of $-\Delta$, it seems reasonable to show its relation to the operator Λ defined in [2]; this operator is defined by $\Lambda = i \sum (\partial/\partial x_m) R_m$, where R_m is the Riesz transform given by

$$R_m f(x) = -i\Gamma(s)\pi^{-s} \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (x_m - y_m) \,|\, x - y \,|^{-k-1} f(y) \, dy, \quad s = \tfrac{1}{2}(k+1).$$

The Fourier transform of R_m is $x_m/|\, x \,|$, so that the transform of Λ is $|\, x \,|$. We show that $(\partial/\partial x_m) I^1 = iR_m$, from which it follows that $I^{-1} = -\Lambda$:

$$\Lambda = i \sum (\partial/\partial x_m) R_m = \sum (\partial/\partial x_m)^2 I^1 = -I^{-2} I = -I^{-1}.$$

To prove $(\partial/\partial x_m) I^1 = iR_m$, let g and f be in C_1 and have compact support. Then

$$\begin{aligned}
-(\partial g/\partial x_m, I^1 f) &= -H(1,k)^{-1} \int \partial g(x)/\partial x_m \int f^*(y) \,|\, x - y \,|^{1-k} \, dy \, dx \\
&= -H^{-1} \int f^*(y) \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial g(x)/\partial x_m) \,|\, x - y \,|^{1-k} \, dx \, dy \\
&= (1-k) H^{-1} \int f^*(y) \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} g(x) \, (x_m - y_m) \,|\, x - y \,|^{-k-1} \, dx \, dy \\
&\qquad + H^{-1} \int f^*(y) \lim_{\epsilon\to 0} \int_{|x-y|=\epsilon} g(x) \gamma_m \, d\sigma_x \, dy;
\end{aligned}$$

here γ_m is the m-th direction cosine and $d\sigma_x$ the measure on the unit sphere, and $x = y + \epsilon\sigma$. Since γ_m has mean value 0 and g is in C_1, the second limit in the last expression is zero, and $-(\partial g/\partial x_m, I^1 f) = (Rg, f)$, where

$$Rg = (1-k) H(1,k)^{-1} \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} g(x) \, (x_m - y_m) \,|\, x - y \,|^{-k-1} \, dx = -iR_m g.$$

Hence $-(\partial g/\partial x_m, I^1 f) = -i(R_m g, f) = (g, iR_m f)$, which is what we were to show.

C. The Green's kernel of $\Delta - \lambda$. We calculate the Green's kernel $E_\lambda(|x-y|)$ of $\Delta-\lambda$ by setting $r=|x-y|$, $E_\lambda(|x-y|)=y(r)$. Then y satisfies

$$y''(r)+\frac{k-1}{r}y'(r)-\lambda y(r)=0, \qquad r>0.$$

Let

$$k=2\nu+2,\ \lambda=\mu^2 \qquad (\mathrm{Re}(\mu)\geqq 0),\ y(r)=r^{-\nu}Y(r).$$

The equation for Y is $r^2Y''+rY'-(\nu^2+r^2\mu^2)Y=0$, which has the singular solution $Y(r)=AK_\nu(\mu r)$, K a modified Bessel function of the second kind. If ν is an integer, $\nu=n$,

$$\begin{aligned} K_\nu(z) = {} & \tfrac{1}{2}\sum_{m=0}^{n-1}(-1)^m(n-m-1)!/\{m!(z/2)^{n-2m}\} \\ & +(-1)^{n+1}\sum_{m=0}^{\infty}\{\log(z/2)-(\tfrac{1}{2})\psi(m+1) \\ & -(\tfrac{1}{2})\psi(n+m+1)\}(z/2)^{n+2m}/\{m!(n+m)!\}. \end{aligned}$$

If ν is $n+\frac{1}{2}$, n an integer, then

$$K_\nu(z)=(\pi/2z)^{\frac{1}{2}}e^{-z}\sum_{r=0}^{n}(n+r)!/\{r!(n-r)!(2z)^r\}$$

([8], p. 80). We choose the constant A in order to have the Green's function for $\Delta-\lambda$, and define

$$E_\lambda(r)=Ar^{-\nu}K_\nu(\mu r),\ \text{where } \nu=(\tfrac{1}{2})k-1, \tag{1}$$

$A=-(\mu/2)^\nu/\nu!\omega_k$ or $A=-1/\omega_2$ according as $k>2$ or $k=2$, and ω_k is the area of the unit sphere in E_k. That this is indeed a Green's kernel for $\Delta-\lambda$ can be checked by applying Green's formula to

$$\int_{|x-y|>\epsilon}E_\lambda(|x-y|)(\Delta-\lambda)f(y)\,dy.$$

From the series for K_ν, we get the following estimates for E_λ:

$$\begin{aligned} & |\,dE_\lambda/dr-\omega_k^{-1}r^{1-k}\,|\leqq C\,|\,\mu\,|\,r^{2-k} \text{ or } C\,|\,\mu\log\mu r\,| \text{ in } |\,\mu r\,|\leqq 1 \\ & \qquad\qquad \text{according as } k>2 \text{ or } k=2, \\ & |\,d^2E_\lambda/dr^2-r^{-k}(1-k)\omega_k^{-1}\,|\leqq C\,|\,\mu\,|\,r^{1-k} \text{ in } |\,\mu r\,|\leqq 1, \\ & d^nE_\lambda/dr^n=A'r^{2-n-k}+O(r^{3-n-k}) \qquad (r\to 0) \end{aligned} \tag{2}$$

generally for fixed λ.

For global estimates consider the integral representation of $K_\nu(z)$ ([8], p. 172):

$$K_\nu(z) = \Gamma(\nu + \tfrac{1}{2})^{-1}\Gamma(\tfrac{1}{2})(\tfrac{1}{2}z)^\nu \int_1^\infty e^{-zt}(t^2 - 1)^{\nu-\frac{1}{2}}\, dt$$

so that, replacing t by $1 + t/\mu r$,

$$E_\lambda(r) = \mu^{2\nu} C \int_1^\infty e^{-\mu r t}(t^2 - 1)^{\nu-\frac{1}{2}}\, dt = C' e^{-\mu r} r^{2-k} \int_0^\infty e^{-t}[t(t + 2\mu r)]^{\nu-\frac{1}{2}}\, dt,$$

where C and C' depend only on k. If we set

$$I_\lambda(r) = \int_0^\infty e^{-t} t^{\frac{1}{2}(k-3)}(t + 2\mu r)^{\frac{1}{2}(k-3)}\, dt$$

with $\mu = \lambda^{\frac{1}{2}}$, $\operatorname{Re}(\mu) \geqq 0$, we have

$$d^n I_\lambda / dr^n = \int_0^\infty e^{-t} 2^{-n}(k-3)\cdots(k-2n-1) t^{\frac{1}{2}(k-3)}(2\mu)^n \ (t + 2\mu r)^{\frac{1}{2}(k-2n-3)}\, dt.$$

If $n \leqq \frac{1}{2}(k-3)$, this is in absolute value $\leqq |\mu|^n P(|\mu| r)$, where P is a polynomial (depending on n and k) with positive coefficients. If k is odd, this holds for all n.

If k is even, $n \geqq \frac{1}{2}(k-3)$, and $r\mu \geqq 0$ then $|d^n I_\lambda / dr^n|$ does not exceed

$$2^{-n} \int_0^\infty e^{-t} |(k-3)\cdots(k-2n-1)| \cdot t^{\frac{1}{2}(k-3)} (2|\mu|)^n (2|\mu| r)^{\frac{1}{2}(k-3)-n}\, dt$$
$$\leqq A r^{-n} (|\mu| r)^{\frac{1}{2}(k-3)}.$$

These estimates lead immediately to

$$(3) \qquad \begin{aligned} &|d^n E_\lambda / dr^n| \leqq |e^{-\mu r}| r^{2-k-n} P_n(|\mu| r) \text{ if } n \leqq \tfrac{1}{2}(k-3) \text{ or } k \text{ is odd;} \\ &|d^n E_\lambda / dr^n| \leqq e^{-\mu r} r^{2-k-n} (\mu r)^{\frac{1}{2}(k-3)} P_n(\mu r) \text{ if } n \geqq \tfrac{1}{2}(k-3) \text{ and } \mu \geqq 0, \end{aligned}$$

where P_n is a polynomial with constant coefficients depending on k and n.

We can use these kernels to construct operators equivalent to the I^α of the previous section for $\alpha \geqq 0$; this will motivate a similar construction on a Riemannian manifold to be given later. Let $\delta > 0$, $k > 2$, and

$$J_\delta^\alpha = (\delta - \Delta)^{-\alpha/2} = \tfrac{1}{2\pi i}\int_C \lambda^{-\alpha/2}(\lambda - \delta + \Delta)^{-1}\, d\lambda = \tfrac{1}{2\pi i}\int_C \lambda^{-\alpha/2} E_{\delta-\lambda}\, d\lambda,$$

where C is the path $\operatorname{Re}(\lambda) = \delta/2$ traversed from top to bottom, and the cut for $\lambda^{-\alpha/2}$ is taken along $\lambda \leqq 0$. From the estimates (3), E_λ is a bounded operator on $L^p(E_k)$, and

$$\| E_\lambda \| \leqq \omega_k \int_0^\infty |E_\lambda(r)| r^{k-1}\, dr \leqq \omega_k \sum a_m \int_0^\infty |e^{-\mu r}| |\mu r|^m r\, dr < A |\lambda|^{-1},$$

($\mathrm{Re}(\lambda) \geqq 0$, $k > 2$) so the integral defining J_δ^α converges in norm if $\alpha > 0$. Since $E_\lambda = (\Delta - \lambda)^{-1}$, its Fourier transform is $-(\lambda + |x|^2)^{-1}$, and the transform of J_δ^α is

$$\hat{J}_\delta^\alpha(x) = \frac{1}{2\pi i}\int_C \lambda^{-\alpha/2}(-|x|^2 - \delta + \lambda)^{-1} d\lambda = (|x|^2 + \delta)^{-\alpha/2},$$

where the root is positive. Thus the J_δ^α form a semi-group of bounded operators on L^2, with $J_\delta^2 = (\delta - \Delta)^{-1}$. J_δ^α converges strongly to the identity as $\alpha \to 0$, since $\hat{J}_\delta^\alpha$ converges boundedly to 1.

We can eliminate the dependence of C on δ, for $0 < \alpha < 2$, by transforming the contour into one surrounding the negative real axis. With this contour Γ we can use the estimates (3) for $k = 2$, and find again $J_\delta^\alpha = (\delta - \Delta)^{-\alpha/2}$, $0 < \alpha < 2$.

From the expression for $\hat{J}_\delta^1$, we see that if f has compact support and is continuous, $J_\delta^1 f$ converges uniformly to $-I^1 f$, where $-I^1$ is the inverse of Λ, discussed in the previous section. Thus $\frac{1}{2\pi i}\int_\Gamma \lambda^{-\frac{1}{2}} E_{-\lambda}(r)\, d\lambda = -H(1,k)^{-1} r^{1-k}$, or

$$\frac{1}{\pi}\int_0^\infty s^{-\frac{1}{2}} E_s(r)\, ds = -H(1,k)^{-1} r^{1-k}. \tag{4}$$

D. The distribution spaces in E_k. The use of Banach space methods in partial differential equations leads naturally to the consideration of spaces of functions whose derivatives are functions in L^p, and to the duals of these spaces.

Definition 2. f is in $L_1^p(E_k)$ if f is in $L^p(E_k)$ and, for every $i = 1, \cdots, k$ there is a function f_i in L^p such that for every ϕ in C_∞ with compact support $-(f, \partial\phi/\partial x_i) = (f_i, \phi)$; or (if $p > 1$), $|(f, \partial\phi/\partial x_i)| \leqq A \|\phi\|_q$, $q^{-1} + p^{-1} = 1$. Then $f_i = (\partial/\partial x_i) f$. f is in L_m^p $(m > 0)$ if f is in L_1^p and all first order derivatives of f are in L_{m-1}^p.

There is a topology in L_m^p defined by the norm

$$\|f\|_m = \Big(\sum_{0 \leqq |\alpha| \leqq m} \|(\partial/\partial x)^\alpha f\|_p^p\Big)^{1/p}.$$

The distribution space L_{-m}^p $(m \geqq 0, 1 < p < \infty)$ is the space of bounded linear functionals on L_m^q, where $p^{-1} + q^{-1} = 1$. $L_0^q = L^q$, $(1 < q < \infty)$.

It is clear that $L_m^p \subset L_{m-1}^p$, $m = 0, \pm 1, \pm 2, \cdots$. Functions in C_∞ with compact support are dense in L_m^p for $m \geqq 0$. (See e.g. [2], Lemma 1.) For $m \geqq 0$, L_m^p is closed under multiplication by bounded functions ϕ in C_m, with bounded derivatives, and $\|\phi f\|_m \leqq C(m) \sup |(\partial/\partial x)^\alpha \phi| \, \|f\|_m$ for $0 \leqq |\alpha| \leqq m$. The same is true for $m < 0$: if h is in L_m^p, then ϕh is the

linear functional on L_{-m}^q defined by $(\phi h, f) = (h, \phi^* f)$, where f is in L_{-m}^q, and (a, b) denotes the value of the functional a on the element b. $h_1 = h_2$ on the compact set C if $\phi h_1 = \phi h_2$ for every ϕ in C_m with support in C.

These spaces play a central role in this paper; the following facts about them will be used frequently.

Remark (a). If H is a C_β^∞ singular integral operator, then H and H^* are bounded on L_m^p for $m \leqq [\beta]$; $(\partial/\partial x_\nu)H - H(\partial/\partial x_\nu)$ and $(\partial/\partial x_\nu)H^* - H^*(\partial/\partial x_\nu)$ are bounded on L_m^p for $m < [\beta]$.

Proof. Write $H = \sum a_{ij} T_{ij}$. Since T_{ij} commutes with differentiation, its norm on L_m^p is bounded by that on L^p. Since a_{ij} is in C_β it is also bounded on L_m^p for $m \leqq [\beta]$, and its norm is $\leqq C(m) \sup_{0 \leqq |\alpha| \leqq m} |(\partial/\partial x)^\alpha a_{ij}|$. Since the supremum on the right is $O(i^{-r})$ for every r, $\| T_{ij} \|$ has a bound independent of i and j, and the number of T_{ij} for fixed i is $O(i^{k-2})$, the series for H can be summed to get $\| H \|_{m,m} < \infty$, where $\| \ \|_{m,m}$ is the norm of an operator from L_m^p to L_m^p. The same method applies to $H^* = \sum T_{ij} a_{ij}^*$,

$$(\partial/\partial x_\nu) H - H(\partial/\partial x_\nu) = \sum (\partial a_{ij}/\partial x_\nu) T_{ij}, \text{ and}$$
$$(\partial/\partial x_\nu) H^* - H^*(\partial/\partial x_\nu) = \sum T_{ij} (\partial a_{ij}/\partial x_\nu)^*.$$

Remark (b). Let $\| K \|_{j,m}$ denote the norm of K as an operator from L_j^p to L_m^p. Suppose $\| K \|_{0,1} < C$ and $\|(\partial/\partial x_i)K - K(\partial/\partial x_i)\|_{m,m} < C$ for $m < n$, $i = 1, \cdots, k$. Then $\| K \|_{m,m+1} < A(m) C$ for $m < n$; all the C's are the same, and $A(m)$ depends only on m and p.

The proof is by induction on m. If f is in L_m^p, $1 \leqq m < n$,

$$\| (\partial/\partial x_i) K f \|_m \leqq \| K \partial f/\partial x_i \|_m + \| ((\partial/\partial x_i) K - K(\partial/\partial x_i)) f \|_m$$
$$\leqq CA(m-1) \| \partial f/\partial x_i \|_{m-1} + C \| f \|_m \leqq CA(m-1) \| f \|_m + C \| f \|_m,$$

so $\| Kf \|_{m+1} \leqq CA(m) \| f \|_m$.

Remark (c). Let T be an operator on L^p for which $(\partial/\partial x_i)T$ and $T(\partial/\partial x_i)$ have some meaning. Then let $C_i(T) = (\partial/\partial x_i)T - T(\partial/\partial x_i)$. If $C_i(T)$ can be similarly combined with differentiation, let $C_j C_i(T) = C_j(C_i(T)) = C_i(C_j(T))$, and generally $C_\alpha(T) = C_1^{\alpha_1} \cdots C_k^{\alpha_k}(T)$. Then if $\| C_\alpha(T) \|_{0,0} < C$ for $|\alpha| < n$, $\| T \|_{m,m} < CA(m)$ for $m < n$.

To see this, let $(\partial/\partial x)^\alpha = (\partial/\partial x_{i_1}) \cdots (\partial/\partial x_{i_m}) = D_1 \cdots D_m$, and $C^\nu(T) = C_{i_\nu}(T)$. Then it can be shown by induction that

$$D_1 \cdots D_m T = T D_1 \cdots D_m + \sum_{\nu=1}^{m} C^\nu(T) D_1 \cdots \not{D}_\nu \cdots D_m$$
$$+ \sum_{1 \leqq \nu < \mu \leqq m} C^\nu C^\mu(T) D_1 \cdots \not{D}_\nu \cdots \not{D}_\mu \cdots D_m + \cdots + C_1 C_2 \cdots C_m(T);$$

here $D_1 \cdots \not{D}_\nu \cdots \not{D}_\mu \cdots D_m$ indicates the product of all the D_i except D_ν and D_μ. Thus if we assume that f is in $L_m{}^p$,

$$D_1 \cdots D_m Tf = TD_1 \cdots D_m f + \cdots + C_1 C_2 \cdots C_m(T) f$$

is in L^p, and $\| Tf \|_m \leqq CA(m) \| f \|_m$.

LEMMA 2. *Let $K(x,y)$ be continuously differentiable for $x \neq y$; $|K(x,y)| < \phi(x-y)$ with $\int \phi(z)\,dz < C$ and $\phi(x) = O(|x|^{1-k})$ as $|x| \to 0$;* and let

$$\lim_{\epsilon\to 0} \epsilon^{k-1} \int_{|x-y|=\epsilon} K(y,x)\gamma_i\, d\sigma_y = -\lim_{\epsilon\to 0} \epsilon^{k-1} \int_{|x-y|=\epsilon} K(x,y)\gamma_i\, d\sigma_y = k_i(x),$$

where $\gamma_i = (y_i - x_i)/|y-x|$ and the first limit exists uniformly in x, and $|k_i| < C$; and if $H(x,y)$ stands for any of the kernels $\partial K(x,y)/\partial y_i$, $\partial K(x,y)/\partial x_i$, $\partial K(y,x)/\partial y_i$, $\partial K(y,x)/\partial x_i$, let $\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} H(x,y) f(y)\, dy$ exist uniformly in x for f in C_1 with compact support, and converge strongly to a bounded operator on L^p. Then

$$\text{(i)} \quad \int K(x,y)(\partial f/\partial y_i)\, dy = -\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial K(x,y)/\partial y_i) f(y)\, dy + k_i(x) f(x), \quad f \text{ in } L_1{}^p$$

$$\text{(ii)} \quad (\partial/\partial x_i) \int K(x,y) f(y)\, dy = \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial K(x,y)/\partial x_i) f(y)\, dy + k_i(x) f(x), \quad f \text{ in } L^p$$

$$\text{(iii)} \quad \int K(x,y)(\partial f/\partial x_i)\, dx = -\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial K(x,y)/\partial x_i) f(x)\, dx - k_i(y) f(y), \quad f \text{ in } L_1{}^p$$

$$\text{(iv)} \quad (\partial/\partial y_i) \int K(x,y) f(x)\, dx = \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial K(x,y)/\partial y_i) f(x)\, dx - k_i(y) f(y), \quad f \text{ in } L^p.$$

Proof. (i) Let f be in C_1 and have compact support. Then

$$\begin{aligned}
&\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} K(x,y)(\partial f/\partial y_i)\, dy \\
&\quad = -\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial K(x,y)/\partial y_i) f(y)\, dy - \lim_{\epsilon\to 0} \int_{|x-y|=\epsilon} \epsilon^{k-1} K(x,y) f(y) \gamma_i\, d\sigma_y \\
&\quad = -\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial K/\partial y_i) f(y)\, dy + k_i(x) f(x).
\end{aligned}$$

The result then holds for f in $L_1{}^p$ by approximation.

(ii) Let g and f be in C_1 and have compact support. Then

$$-(\partial g/\partial x_i, \int K(x,y)f(y)\,dy) = -\int f^*(y) \int (\partial g/\partial x_i)K^*(x,y)\,dx\,dy$$
$$= \int f^*(y)\{\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon} g(x)\,(\partial K^*/\partial x_i)\,dx + k_i{}^*(y)g(y)\}dy \quad \text{(by (i))}$$
$$= \lim_{\epsilon\to 0}\int\int_{|x-y|>\epsilon} f^*(y)g(x)\,(\partial K^*/\partial x_i)\,dy\,dx + \int k_i{}^*f^*g(y)\,dy$$
$$= \int g(x)\{\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon} f^*(y)\,(\partial K^*/\partial x_i)\,dy + k_i{}^*(x)f^*(x)\}dx.$$

Hence if f is in C_1 with compact support, $\int K(x,y)f(y)\,dy$ has the (weak) derivative given in (ii); the result holds again by approximation for f in L^p.

(iii) and (iv) follow from (i) and (ii) respectively.

We introduce as a notational convenience $(\partial/\partial x_i + \partial/\partial y_i)f(x,y) = \partial f/\partial x_i + \partial f/\partial y_i$, and $(\partial/\partial x + \partial/\partial y)^\alpha f(x,y) = \prod(\partial/\partial x_i + \partial/\partial y_i)^{\alpha_i}f(x,y)$.

LEMMA 3. *If $K(x,y)$ has continuous derivatives up to and including order n for $y \neq x$, and $(\partial/\partial x + \partial/\partial y)^\alpha K(x,y)$ satisfies for $|\alpha| < n$ all the conditions imposed on K in Lemma 2, and for every $i = 1,\cdots,k$, then $\| K \|_{m,m+1} < A(n,p)B$ and $\| K^* \|_{m,m+1} < A(n,p)B$ for $m < n$; B is an upper bound for the C of Lemma 2, $\| K \|_{0,1}$ and $\| K^* \|_{0,1}$.*

Proof. Let $(\partial/\partial x_j)K - K(\partial/\partial x_j) = K_j$; by Lemma 2, K_j is the operator with kernel $(\partial/\partial x_j + \partial/\partial y_j)K(x,y) = K_j(x,y)$. Then $(\partial/\partial x + \partial/\partial y)^\alpha K_j(x,y)$ satisfies for $|\alpha| < n-1$ the conditions on K in Lemma 2. An easy induction then shows that for $|\alpha| < n$, $C_\alpha(K_j)$ is the operator with kernel

$$(\partial/\partial x + \partial/\partial y)^\alpha K_j(x,y), \text{ and } \| C_\alpha(K_j) \|_{0,0} < B$$

By Remark (c), $\| K \|_{m,m} < BA(m)$ for $m < n$. By Lemma 2, $\| K \|_{0,1} < B$, so that Remark (b) gives $\| K \|_{m,m+1} < A(n,p)B$ for $m < n$.

Since the conditions on the kernel of K^* are the same as those on K, $\| K^* \|_{m,m+1} < A(n,p)B$ for $m < n$.

COROLLARY. *Let $H(x,z)$ be in $C_\beta{}^\infty$ and homogeneous of degree $1-k$ in z; $\theta(x,y)$ be in C_β on E_{2k} with $|\theta(x,y)| < \phi(x-y)$, where ϕ is bounded and $\phi(x) = 0$ for $|x| > R$. Then if K is the operator with kernel*

$$\theta(x,y)H(x,x-y), \text{ we have } \| K \|_{m,m+1} < A \text{ and } \| K^* \|_{m,m+1} < A$$

for $m < [\beta]$.

Proof. Let $H_\alpha(x,z) = (\partial/\partial x)^\alpha H(x,z)$. Then

$$
\begin{aligned}
&(\partial/\partial x + \partial/\partial y)^\alpha \theta(x,y) H(x, x-y) \\
&\quad = (\partial/\partial \xi)^\alpha \theta(\tfrac{1}{2}(\xi+\eta), \tfrac{1}{2}(\xi-\eta)) H(\tfrac{1}{2}(\xi+\eta), \eta) \\
&\quad = \sum_{\gamma \leqq \alpha} \{\alpha!/\gamma!(\alpha-\gamma)!\} (\partial/\partial\xi)^\gamma \theta(\tfrac{1}{2}(\xi+\eta), \tfrac{1}{2}(\xi-\eta)) (\partial/\partial\xi)^{\alpha-\gamma} \\
&\qquad\qquad \times H(\tfrac{1}{2}(\xi+\eta), \eta) \\
&\quad = \sum_{\gamma \leqq \alpha} \{\alpha!/\gamma!(\alpha-\gamma)!\} (\partial/\partial x + \partial/\partial y)^\gamma \theta(x,y) 2^{-|\alpha-\gamma|} H_{\alpha-\gamma}(x, x-y).
\end{aligned}
$$

Hence we need only show that if $\theta(x,y)$ is in C_1, $|\theta(x,y)| < \phi(x-y)$ with ϕ bounded and of compact support, and if $H(x,z)$ is in C_1^∞ and homogeneous of degree $1-k$ in z, then θH satisfies the conditions of Lemma 2. The first one is obvious. For the second,

$$
\begin{aligned}
&-\lim_{\epsilon\to 0} \epsilon^{k-1} \int_{|x-y|=\epsilon} \theta(x,y) H(x, x-y) ((y_i - x_i)/|y-x|) \, d\sigma_y \\
&\quad = \lim_{\epsilon\to 0} \epsilon^{k-1} \int_{|z|=\epsilon} \theta(x, x-z) H(x,z) (z_i/|z|) \, d\sigma_z = \theta(x,x) \int_{|z|=1} H(x,z) z_i \, d\sigma_z.
\end{aligned}
$$

In the same way,

$$
\begin{aligned}
&\lim_{\epsilon\to 0} \epsilon^{k-1} \int_{|x-y|=\epsilon} \theta(y,x) H(y, y-x) ((y_i - x_i)/|y-x|) \, d\sigma_y \\
&\qquad = \theta(x,x) \int_{|z|=1} H(x,z) z_i \, d\sigma_z.
\end{aligned}
$$

For the last condition we take as an example the kernel

$$
(\partial/\partial x_i) \{\theta(x,y) H(x, x-y)\}.
$$

Let

$H_i(x,z) = \partial H(x,z)/\partial x_i$, $H^i(x,z) = \partial H(x,z)/\partial z_i$, and $\theta_i(x,y) = \partial\theta(x,y)\partial x_i$.

Then the limit that concerns us is

$$
\begin{aligned}
&\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} \{\theta_i(x,y) H(x, x-y) + \theta(x,y) H_i(x, x-y)\} f(y) \, dy \\
&\qquad + \lim_{\epsilon\to 0} \int_{\epsilon<|x-y|<R} \{\theta(x,y) - \theta(x,x)\} H^i(x, x-y) f(y) \, dy \\
&\qquad + \lim_{\epsilon\to 0} \int_{R>|x-y|>\epsilon} \theta(x,x) H^i(x, x-y) f(y) \, dy.
\end{aligned}
$$

The kernel in each of the first two integrals is dominated by $\psi(x-y)$ for some ψ in L^1, so that they converge uniformly for bounded f, and define bounded operators on L^p. The last operator is a truncated C_β^∞ singular

integral operator, by Lemma 1, and it follows from the results in [1] that this is a bounded operator on L^p. It converges uniformly for f in C_1 since

$$\lim_{\epsilon\to 0}\int_{R>|x-y|>\epsilon}\theta(x,x)H^i(x,x-y)f(y)\,dy$$
$$=\lim_{\epsilon\to 0}\int_{R>|x-y|>\epsilon}\theta(x,x)H^i(x,x-y)\{f(y)-f(x)\}\,dy;$$

this integrand is dominated by a $\psi(x-y)$ with ψ in L^1.

PROPOSITION. *$L_m{}^p$ is topologically isomorphic to $L_{m+1}{}^p$, $1<p<\infty$.*

Proof. The isomorphism is defined for $m\geqq 0$ by

$$G(f)=(I-i\Lambda)(I-\Delta)^{-1}f,$$

where Λ is as in section B above. We will prove that G maps $L_m{}^p$ continuously into $L_{m+1}{}^p$; one sees from the Fourier transforms that $(I+i\Lambda)G$ and $G(I+i\Lambda)$ are the identity operators on $L_m{}^p$ and $L_{m+1}{}^p$ respectively. Since Λ and the Riesz transform R_j commute with differentiation, and R_j is bounded on $L_m{}^p$, $(m\geqq 0)$, Λ maps $L_m{}^p$ continuously into $L_{m-1}{}^p$ for $m>0$, so that G^{-1} is bounded from $L_{m+1}{}^p$ to $L_m{}^p$.

We show that G is defined and continuous from $L_m{}^p$ into $L_{m+1}{}^p$ by proving that the Green's function of $\Delta-1$ maps $L_m{}^p$ into $L_{m+2}{}^p$. The Green's function is, from (1), $E_1(|x-y|)=B\,|x-y|^{1-\frac{1}{2}k}K_{\frac{1}{2}k-1}(|x-y|)$. Let f be in L^p. Then by Lemma 2

$$(\partial/\partial x_i)(\Delta-1)^{-1}f=\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}(\partial E_1/\partial x_i)f(y)\,dy$$
$$-f(x)\lim_{\epsilon\to 0}\epsilon^{k-1}\int_{|x-y|=\epsilon}E_1(|x-y|)\gamma_i\,d\sigma_y=\int(\partial E_1/\partial x_i)f(y)\,dy,$$

since $E_1(r)$ is $O(r^{2-k})$ and $E_1'(r)=O(r^{1-k})$. Then again

$$(\partial^2/\partial x_i\partial x_j)(\Delta-1)^{-1}f=\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}(\partial^2E_1/\partial x_i\partial x_j)f(y)\,dy$$
$$-f(x)\lim_{\epsilon\to 0}\int_{|x-y|=\epsilon}(\partial E_1/\partial x_i)\gamma_j\epsilon^{k-1}\,d\sigma_y.$$

Since $\partial\,|x-y|/\partial x_i=-(y_i-x_i)/|y-x|=-\gamma_i$, (2) shows that this last limit is $(\delta_{ij}/k)f(x)$. To show $\partial^2E_1/\partial x_i\partial x_j$ is summable as required in Lemma 2, write it as

$$X(|x-y|)A\partial^2\,|x-y|^{2-k}/\partial x_i\partial x_j$$
$$+X(|x-y|)\partial^2\{E_1(|x-y|)-A\,|x-y|^{2-k}\}/\partial x_i\partial x_j$$
$$+\{1-X(|x-y|)\}\partial^2E_1/\partial x_i\partial x_j,$$

where $X(t)=1$ if $t<1$ and $X(t)=0$ if $t>1$. That the first term is summable is proved in [1], and the last two are in L^1, according to the estimates (2) and (3).

This shows that $(\Delta-1)^{-1}$ is bounded from L^p to $L_2{}^p$. Since it commutes with differentiation, it is also bounded from $L_m{}^p$ to $L_{m+2}{}^p$.

This argument is not exactly right for $k=2$, but the modifications are trivial.

Now that the proposition is proved for $m\geqq 0$, it is seen to be true for all m. A consequence of this is that $L_m{}^p$ is isomorphic to L^p, and hence reflexive, for $\infty>p>1$.

Operators which add to the number of derivatives of a function in L^p are in some sense "smoothing" operators. This can be made precise.

Definition 3. T is smoothing of order n if T is a bounded transformation of $L_m{}^p$ into $L_{m+1}{}^p$ for $-n\leqq m<n$. Equivalently, T is defined on L^p and bounded from $L_m{}^p$ to $L_{m+1}{}^p$ $(0\leqq m<n)$; and T^* is bounded from $L_m{}^q$ to $L_{m+1}{}^q$ $(0\leqq m<n)$.

For example, the operator $(I-i\Lambda)(I-\Delta)^{-1}$ of the previous proposition is smoothing of order n for every n.

II. Singular Integral Operators on a Compact Manifold.

Throughout this section, unless otherwise specified, M will denote a compact manifold of dimension k, class C_n, $(n\geqq 3)$. The singular integral operators will be characterized by their local behavior. The conventions of tensor calculus will generally not be used.

A. The functional spaces on M. We can define $L_r{}^p(M)$ $(1<p<\infty$, $r\leqq n)$ as a topological vector space by using a partition of the identity on M in the form of a finite collection $\{\phi_i\}$ of functions in C_n satisfying

i) $\phi_i\geqq 0$, $\sum\phi_i=1$;

ii) the support of ϕ_i lies in the domain of a single coordinate system.

With each ϕ_i we can associate a particular coordinate system x^i. Then if f is a function defined almost everywhere in each coordinate domain, $\phi_i f$ can be considered as a function of compact support in E_k. We say that f is in $L_r{}^p(M)$ if $\phi_i f$ is in $L_r{}^p(E_k)$ for each i. If $\|\ \|$ denotes the norm on $L^p(E_k)$, then we define a topology on $L_r{}^p(M)$ by the norm

$$\|f\|_{r,p}=\Big(\sum_{|\alpha|\leqq r}\sum_i\|\phi_i^{1/p}(\partial/\partial x_i)^\alpha f\|^p\Big)^{1/p}.$$

When $r=0$, this is $L^p(M, v)$, where v is the measure $\sum \phi_i dx^i$. The identification of functionals on L^p as functions in L^q can be made using the inner product given by this measure.

It should be checked that the norms obtained with different coordinate systems and different $\{\phi_i\}$ are all equivalent. Suppose first that $x(\xi)$ is a coordinate change in U_i, the support of ϕ_i. Then if f is in $L_m{}^p$ (in the ξ system), and $|\alpha| \leqq m$, $(\partial/\partial x)^\alpha f = \sum_{|\beta| \leqq |\alpha|} c_\beta (\partial/\partial \xi)^\beta f$, where the c_β are bounded functions. Thus the norm from the x system is dominated by that of the ξ system; and they are seen to be equivalent by reversing the roles of x and ξ. To show independence of the choice of $\{\phi_i\}$, we need only consider the case where the second system is of the form $\{\phi_{ij}\}$ with $\sum_j \phi_{ij} = \phi_i$, and using a single coordinate system in U_i. Then

$$(\sum_{i,j,\alpha} \| \phi_{ij}{}^{1/p} (\partial/\partial x)^\alpha f \|^p)^{1/p} = (\sum_{i,\alpha} \| \phi_i{}^{1/p} (\partial/\partial x)^\alpha f \|^p)^{1/p}.$$

The distribution space $L_{-r}{}^p(M)$ is defined, as in the Euclidean case, to be the dual of $L_r{}^p$. It will be a corollary of some later results that these spaces are isomorphic to $L^p(M)$, hence reflexive, for $1 < p < \infty$.

A smoothing operator of order m is an operator T on $L^p(M)$ such that T maps $L_r{}^p$ continuously into $L_{r+1}{}^p$ and T^* maps $L_r{}^q$ continuously into $L_{r+1}{}^q$ for $0 \leqq r < m$. T is such an operator if and only if, for every ϕ and ψ in C_n with support in a single coordinate neighborhood, $\phi T \psi$, considered as an operator on $L^p(E_k)$, is smoothing of order m.

B. Singular integral operators on M and their symbols.

Definition 4. An operator T defined on $L^p(M)$ is of type $C_\beta{}^\infty$ ($\beta \leqq n-1$) if it satisfies

i) for each ϕ and ψ in C_n on M with disjoint (compact) support, $\phi T \psi$ is completely continuous and smoothing of order $[\beta]$ on all $L^p(M)$, $1 < p < \infty$;

ii) for each ϕ and ψ in C_n with support in a common coordinate domain with coordinates x, $\phi T \psi = \phi H \psi + R$, where H is a Euclidean $C_\beta{}^\infty$ singular integral operator

$$Hf(x) = a(x)f(x) + \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h(x, x-y) f(y)\, dy,$$

and R is completely continuous and smoothing of order $[\beta]$ on $L^p(M)$, $1 < p < \infty$.

Definition 5. The symbol of a C_β^∞ operator T on M is the function on the cotangent bundle of M defined by

$$\sigma(T)(p, \sum \xi_i\, dx_i) = a(x(p)) + \lim_{\epsilon\to 0} \int_{\epsilon^{-1}>|\eta|>\epsilon} \exp(i \sum \xi_j\eta_j) h(x(p), \eta)\, d\eta$$

where $a(x)$ and $h(x,\eta)$ are the functions in Definition 4, $\eta = (\eta_1, \cdots, \eta_k)$, $|\eta|^2 = \sum \eta_i^2$, and p is in the common support of ϕ and ψ.

The existence of such operators will be established in Theorem 2 below, and the independence of symbols and coordinate systems in Theorem 1.

Spherical harmonics provide a useful link between the operator T and its symbol $\sigma(T)$. If $h(x,z) = \sum a_{nm}(x) Y_{nm}(z) |z|^{-k}$, the Euclidean symbol of the operator $H = a + \int h$ is

$$a(x) + \lim_{\epsilon\to 0} \int_{\epsilon^{-1}>|\zeta|>\epsilon} \exp(i \sum z_j\zeta_j) h(x,\zeta)\, d\zeta = a(x) + \sum a_{nm}(x)\gamma_n Y_{nm}(z),$$

wherein $\gamma_n = i^n\pi^{k/2}\Gamma(n/2)/\Gamma(\frac{1}{2}\{n+k\})$. For this see [2].

If H is the operator of Definition 4, then

$$\sigma(T)(p, \sum \xi_i\, dx_i) = a(x(p)) + \sum a_{nm}(x(p))\gamma_n Y_{nm}(\xi),$$

where ξ is the point in E_k with coordinates $(\xi_1, \cdots, \xi_k)$. Thus the symbol of a C_β^∞ operator is a function on the cotangent bundle which is homogeneous of degree zero on each cotangent space, and in C_∞ with respect to cosphere variables; and each derivative with respect to these variables is in C_β on the cosphere bundle. Such a function will be called a C_β^∞ function on the cosphere bundle $CS(M)$.

LEMMA 4. *If $\phi T\psi - \phi H_1\psi$ and $\phi T\psi - \phi H_2\psi$ are both completely continuous, then $\sigma(H_1)(x(p),z) = \sigma(H_2)(x(p),z)$ if p is in the common support of ϕ and ψ.*

THEOREM 1. *The symbol $\sigma(T)$ is independent of the coordinates used to define it.*

Proof of Lemma 4. By our hypotheses, $\phi(H_1 - H_2)\psi$ is a completely continuous operator on $L^p(E_k)$. Let U be the common support of ϕ and ψ (considered as a subset of E_k). Let $L^p(U)$ be the functions in $L^p(E_k)$ which vanish off U. Consider the vector space C of symbols of (Euclidean) C_0^∞ operators with the property that $\sigma(H)(x,z)$ vanishes off U, and H is completely continuous on $L^p(U)$. We will see that $\sigma\{\phi\psi(H_1 - H_2)\}$ is in C, and that C is trivial.

First, let $a(x)$ and $b(x)$ have compact support, $a(x)$ in C_0 and $b(x)$ in C_1;

and let $h(x,z)$ be a $C_0{}^\infty$ kernel. Then $a(x)\{b(x)-b(y)\}h(x,x-y)$ is uniformly $O(|x-y|^{1-k})$, hence defines a completely continuous operator $a(bH-Hb)$ on $L^p(U)$. But any b in C_0 can be approximated uniformly by functions in C_1, so that $a(bH-Hb)$ is approximated in norm by completely continuous operators if $a(x)$ and $b(x)$ are only continuous. Thus $\phi\psi(H_1-H_2)$ $=\phi(H_1-H_2)\psi+\phi\{\psi(H_1-H_2)-(H_1-H_2)\psi\}$ has a symbol in C.

Now let Y_{nm} be a normalized spherical harmonic, and

$$T_{nm}f(x)=\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}Y_{nm}(x-y)f(y)\,dy.$$

Then if $\sigma(H)$ is in C, K is a $C_0{}^\infty$ operator, $H=\sum a_{nm}T_{nm}$, $K=\sum b_{nm}T_{nm}$ (the b_{nm} having support in U) and $H\circ K$ is the $C_0{}^\infty$ operator with symbol $\sigma(H)\sigma(K)$, we have $H\circ K=HK-\sum a_{nm}(T_{nm}b_{\nu\mu}-b_{\nu\mu}T_{nm})T_{\nu\mu}$. Then as in the previous paragraph $a_{nm}(T_{nm}b_{\nu\mu}-b_{\nu\mu}T_{nm})$ is completely continuous on $L^p(U)$, so that $H\circ K$ is also. Thus C is closed under multiplication by $C_0{}^\infty$ functions $F(x,z)$, homogeneous of degree zero in z, vanishing for x not in U.

Now suppose $F(x_0,z)$ is not identically zero in z, but $F(x,z)$ is in C. Let $\theta(x_0)=1$, and θ vanish outside a spherical neighborhood of x_0 in U, and $F'(x,z)=\theta(x)F(x,z)$. Let u be a rotation of E_k about x_0, and $F_u(x,z)=F'(u(x),u(x_0+z)-x_0)$. Then F_u is also clearly in C; and we can find finitely many u_i so that $G(x,z)=\sum|F_{u_i}(x,z)|^2$ is bounded away from zero in a neighborhood of x_0. Let $a(x)$ be continuous and have support in this neighborhood. Then $a(x)G(x,z)^{-1}z_j|z|^{-1}$ is in $C_0{}^\infty$ and $a(x)G(x,z)^{-1}z_j|z|^{-1}G(x,z)=a(x)z_j|z|^{-1}$ is in C. But $z_j|z|^{-1}$ is the symbol of the Riesz transform R'_j and so aR_j is completely continuous on $L^p(U)$. Then $a^2I=\sum(aR_j)^2+\sum a(aR_j-R_ja)R_j$ is completely continuous. This contradiction establishes Lemma 4.

As a consequence, the H appearing in part (ii) of Definition 4 is essentially unique. We need two more results to establish Theorem 1.

LEMMA 5. *Let $h(x,z)$ be a $C_\beta{}^\infty$ function, homogeneous of degree $-k$, $\beta\geqq 0$, and $\xi(x)$ a C_n change of coordinates. Let $\rho^2(x,y)=\sum\{\xi_i(x)-\xi_i(y)\}^2$, $H_\epsilon f(x)=\int_{|x-y|>\epsilon}h(x,x-y)f(y)\,dy$, and $H_\epsilon'f(x)=\int_{\rho(x,y)>\epsilon}h(x,x-y)f(y)\,dy$, f in $L^p(E_k)$. Then $H_\epsilon f$ and $H_\epsilon'f$ have limits Hf and $H'f$ respectively, as $\epsilon\to 0$, and $H'f(x)-Hf(x)=D(x)f(x)$, where*

$$D(x)=-\int_{|z|=1}h(x,z)\log b(x,z)\,d\sigma \text{ and } b(x,z)=\lim_{t\to 0}t/\rho(x,x+tz).$$

$D(x)$ is in $C_{n-1}\cap C_\beta$.

Proof. As $t \to 0$,

$$b^{-2}(x,z) = \lim \rho^2(x, x+tz)/t^2 = \lim \sum(\{\xi_i(x+tz) - \xi_i(x)\}/t)^2$$
$$= \sum_i \{\sum_j (\partial\xi_i/\partial x_j)(x) z_j\}^2,$$

so $b(x,z)$ is in C_{n-1}. Now for f in C_1 with compact support

$$\text{i)} \qquad H_\epsilon' f(x) = \int_{\substack{\rho(x,y)>\epsilon \\ |x-y|\leqq 1}} h(x, x-y)\{f(y) - f(x)\} dy$$
$$+ f(x) \int_{\substack{\rho(x,y)>\epsilon \\ |x-y|\leqq 1}} h(x, x-y)\, dy + \int_{|x-y|>1} h(x, x-y) f(y)\, dy.$$

The first term is convergent and the limit of the first and last terms together is $\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} h(x, x-y) f(y)\, dy = Hf(x)$. To calculate the second, let $b(\epsilon, x, z)$ be defined for $|z| = 1$ and small ϵ by $\rho(x, x+zb(\epsilon, x, z)) = \epsilon$; and let $m(\epsilon, x) = \max_{|z|=1} b(\epsilon, x, z)$. Then

$$\int_{\rho(x,y)>\epsilon} h(x, x-y)\, dy = \int_{|z|=1} \int_{b(\epsilon,x,z)}^{m(\epsilon,x)} h(x, tz) t^{k-1}\, dt\, d\sigma$$
$$= \int_{|z|=1} h(x,z) \log\{m(\epsilon, x)/b(\epsilon, x, z)\} d\sigma.$$

Now

$$\lim_{\epsilon\to 0} b(\epsilon, x, z)/\epsilon = \lim_{b\to 0} b/\rho(x, x+zb) = b(x,z),$$

so

$$\lim m(\epsilon, x)/b(\epsilon, x, z) = \{\max_{|z|=1} b(x,z)\}/b(x,z),$$

and

$$\lim_{\epsilon\to 0} \int_{\rho(x,y)>\epsilon} h(x, x-y)\, dy = -\int_{|z|=1} h(x,z) \log b(x,z)\, d\sigma = D(x).$$

Hence (i) approaches the desired expression as $\epsilon \to 0$, pointwise and in L^p norm. The same result holds also for f in L^p by approximation, and Lemma 3 is proved.

Note that $b(x,z)$ is even in z, so that if $h(x,z)$ is odd in z, the method of summation is irrelevant.

LEMMA 6. *Let $x(\xi)$ be a C_n change of coordinates $(n \geqq 3)$ in a neighborhood U of E_k. Let $x(\xi) = x$, $x(\eta) = y$, $a_{ij} = (\partial x_i/\partial \xi_j)$, $A = (a_{ij})$. Let $h(x,z)$ be in C_β^∞, $0 \leqq \beta \leqq n-1$, and homogeneous of degree $-k$. Then $h(x, x-y) = h(x, A(\xi - \eta)) + R(\xi, \eta)$, where $R(\xi, \eta)$ is uniformly*

$O(|\xi-\eta|^{1-k})$. *If* $1 \leqq \beta \leqq n-1$, *then* $\phi(\xi)\psi(\eta)R(\xi,\eta)$ *defines an operator which is smoothing of order* $[\beta]$ *on* $L^p(U)$ *for every* ϕ *and* ψ *in* C_{n-1} *with support in* U.

Proof. By Taylor's expansion,

$$\begin{aligned} x_i(\eta) &= \sum_{0\leqq|\alpha|<3} x_i^{(\alpha)}(\xi)\,(1/\alpha!)\,(\eta-\xi)^\alpha - P_i(\xi,\eta) \\ &= x_i(\xi) + \sum_j a_{ij}(\eta_j-\xi_j) - Q_i(\xi,\eta) - P_i(\xi,\eta). \end{aligned}$$

$P_i(\xi,\eta) = O(|\xi-\eta|^3)$ and any first order derivative of $P_i(\xi,\eta)$ is $O(|\xi-\eta|^2)$. Now let

$$Q = \{Q_1(\xi,\eta),\cdots,Q_k(\xi,\eta)\}, \qquad P = \{P_1(\xi,\eta),\cdots,P_k(\xi,\eta)\},$$
$$\text{and } h^{(\alpha)}(x,z) = (\partial/\partial z)^\alpha h(x,z).$$

Then

$$\begin{aligned} h(x,x-y) &= h(x,A(\xi-\eta)+Q+P) \\ &= h(x,A(\xi-\eta)) + \sum_{|\alpha|=1} Q^\alpha h^{(\alpha)}(x,A(\xi-\eta)) + \sum_{|\alpha|=1} P^\alpha h^{(\alpha)}(x,A(\xi-\eta)) \\ &\quad + |A(\xi-\eta)|^{-k-2}\sum_{|\alpha|=2}(Q+P)^\alpha \int_0^1 (1-t)h^{(\alpha)}(x,|A(\xi-\eta)|^{-1} \\ &\qquad \times\{A(\xi-\eta)+t(Q+P)\})\,dt \\ &= h(x,A(\xi-\eta)) + h_1(\xi,\xi-\eta) + R_1(\xi,\eta) + R_2(\xi,\eta). \end{aligned}$$

Here $h_1(\xi,z)$ is homogeneous of degree $1-k$, R_1 and R_2 are uniformly $O(|\xi-\eta|^{2-k})$, and any first derivative of R_1 or R_2 is uniformly $O(|\xi-\eta|^{1-k})$.

Then by Lemma 2 and the Corollary of Lemma 3,

$$\phi(x)\{h_1(\xi,\xi-\eta)+R_1(\xi,\eta)+R_2(\xi,\eta)\}\psi(y) = \phi R\psi$$

is a bounded operator from L^p to L_1^p. To show boundedness from L_m^p to L_{m+1}^p for $m<[\beta]$, note that $\phi R\psi$ measures the difference between

$$\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}\phi(x)h(x,x-y)\psi(y)f(y)\,dy \text{ and}$$

$$\lim_{\epsilon\to 0}\int_{|\xi-\eta|>\epsilon}\phi(x(\xi))h_0(\xi,\xi-\eta)\psi(x(\eta))f(\eta)\det(\partial x_i/\partial\eta_j)\,d\eta$$
$$+\phi(x(\xi))\psi(x(\xi))D(\xi)f(\xi),$$

where $D(\xi)$ is in C_β as in Lemma 5. It is a trivial modification of Remark (a) that the difference between these two operators, $\phi R\psi$, satisfies $\|(\partial/\partial x_i)\phi R\psi - \phi R\psi(\partial/\partial x_i)\|_{m,m} < C$, and the same for the adjoint; then by Remark (b), $\|\phi R\psi\|_{m,m+1} < C$ and $\|\psi^* R^* \phi^*\|_{m,m+1} < C$ for $m < [\beta]$.

Proof of Theorem 1. By Lemma 4, the operator H in Definition 4 is determined by the coordinate system. We call this the principal part of T in the coordinate system x. Let $x(x^*)$ be a C_n change of coordinates, $x(x^*) = x$, $x(y^*) = y$. By Lemmas 5 and 6, writing v for $\det(a_{ij})$,

$$\begin{aligned}
Hf(x) &= a(x)f(x) + \lim_{\epsilon\to 0}\int_{|x-y|>\epsilon} h(x, x-y)f(y)\,dy \\
&= a(x)f(x) - D(x)f(x) + \lim_{\epsilon\to 0}\int_{|x^*-y^*|>\epsilon} h(x, x-y)f(y)\,dy \\
&= a(x)f(x) - D(x)f(x) + \lim_{\epsilon\to 0}\int_{|x^*-y^*|>\epsilon} v(x^*)h(x, A(x^*-y^*))f(y)\,dy^* \\
&\quad + \int h(x, A(x^*-y^*))\{v(y^*)-v(x^*)\}f(y)\,dy^* \\
&\quad + \int R(x^*, y^*)f(y)v(y^*)\,dy^*.
\end{aligned}$$

Since $\phi(x^*)h(x(x^*), A(x^*-y^*))\{v(y^*)-v(x^*)\}\psi(y^*) = O(|x^*-y^*|^{1-k})$, it defines a completely continuous operator. Thus the principal part of T in the coordinate system x^* is the operator

$$\begin{aligned}
H'f(x^*) &= a(x(x^*))f(x^*) - D(x(x^*))f(x^*) \\
&\quad + \lim_{\epsilon\to 0}\int_{|x^*-y^*|>\epsilon} v(x^*)h(x(x^*), A(x^*-y^*))f(y^*)\,dy^*.
\end{aligned}$$

If we use this to compute the symbol, letting $\sum \xi_i dx_i = \sum \xi_i^* dx_i^*$, $\eta = A(\eta^*)$, we find

$$\begin{aligned}
\sigma(T)(p, \textstyle\sum \xi_i^* dx_i^*) &= a(x(p)) - D(x(p)) \\
&\quad + \lim_{\epsilon\to 0}\int_{|\eta^*|>\epsilon} \exp\{i \textstyle\sum \xi_j^*\eta_j^*\} h(x(p), A\eta^*)v(x^*)\,d\eta^* \\
&= a - D + \lim_{\epsilon\to 0}\int_{|\eta^*|>\epsilon} \exp\{i\textstyle\sum \xi_j\eta_j\} h(x(p), \eta)\,d\eta \\
&= a - D + \lim_{\epsilon\to 0}\int_{|\eta|>\epsilon} \exp\{i\textstyle\sum \xi_j\eta_j\} h(x(p), \eta)\,d\eta + D.
\end{aligned}$$

This proves Theorem 1.

THEOREM 2. *The correspondence of singular integral operators of type C_β^∞ with their symbols is a vector space homomorphism of the set of these operators onto the set of C_β^∞ functions on $CS(M)$.*

Proof. The only statement that needs to be proved is the fact that the homomorphism is onto. Let $F(p, \xi)$ be a C_β^∞ function on $CS(M)$. Let $\{\phi_i\}$

be a resolution of the identity as in section II-A above: $\sum \phi_i(p) = 1$, $0 \leqq \phi_i$, ϕ_i is in C_n and has support in a single coordinate neighborhood U_i. Let $\psi_i = 1$ on the support of ϕ_i, and have support in U_i, and let ψ_i be in C_n. Let x be a coordinate system in U_i. Then in terms of the basis $\{dx_i\}$ we can write, with $\xi = \sum \xi_i dx_i$ on the left, $\xi = (\xi_1, \cdots, \xi_k)$ on the right,

$$F(p, \xi) = a(p) + \sum b_{nm}(p) Y_{nm}(\xi).$$

Let $h(x, z) = \sum b_{nm}\gamma_n^{-1} Y_{nm}(z) \mid z \mid^{-k}$. Then set

$$T_i f(x) = \phi_i(x) \{a(x) f(x) + \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h(x, x-y) \psi_i(y) f(y)\, dy\}.$$

The symbol of T_i is then $\phi_i F$, and the symbol of $\sum T_i$ is F. This proves Theorem 2.

Note that if L^p is given the norm $\| f \| = (\sum \| \phi_i^{1/p} f \|^p)^{1/p}$, then $\| \sum T_i f \| \leqq AM \| f \|$, where A is a constant depending on p, $\{\phi_i\}$, and the coordinate systems chosen, and M is an upper bound for F and its derivatives of order $2k$ with respect to cosphere variables. (See [2], Theorem 3).

C. Functional calculus of symbols.

THEOREM 3. *Let $\beta \neq 1$. Then* i) *if T is a C_β^∞ operator, so is T^*, and $\sigma(T^*) = \sigma(T)^*$;* ii) *if $\sigma(T_1)\sigma(T_2) = \sigma(T)$, then $T - T_1T_2$ is completely continuous and smoothing of order $[\beta]$.*

Proof. Let v be the volume element used to define the correspondence between L^q and the dual of L^p. Then $(\phi T \psi)^* = \psi^* H^* \phi^* + R^*$ (see Definition 4), and for f in L^q,

$$H^* f(x) = a^*(x) f(x) + \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} v(y) v(x)^{-1} h^*(y, y-x) f(y)\, dy.$$

Now if $h(x, z) = \sum a_{nm}(x) Y_{nm}(z) \mid z \mid^{-k}$, then

$$\sigma(T)(p, \sum \xi_i dx_i) = a(x(p)) + \sum a_{nm}(x(p)) \gamma_n Y_{nm}(\xi)$$

and

$$\sigma(T)^* = a^* + \sum a_{nm}^* \gamma_n^* Y_{nm}(\xi) = a^* + \sum a_{nm}^* \gamma_n Y_{nm}(-\xi)$$

(for Y_{nm} is odd when n is odd, and even when n is even). The singular kernel associated with this symbol and this coordinate system is

$$H^\# f(x) = a^*(x) f(x) + \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h^*(x, y-x) f(y)\ dy.$$

Thus it must be shown that

$$\lim_{\epsilon \to 0} \phi(x) v(x)^{-1} \int_{|x-y|>\epsilon} v(y) h^*(y, y-x) \psi(y) f(y)\, dy$$

differs by a completely continuous operator, smoothing of order $[\beta]$, from $\phi(x)\lim_{\varepsilon\to 0}\int_{|x-y|>\varepsilon} h^*(x,y-x)f(y)\psi(y)\,dy$. This is done by reverting again to spherical harmonics and the operators T_{nm}, as above. That $\phi\{cT_{nm}-T_{nm}c\}$ is completely continuous is proved above. That it is smoothing for $\beta>1$ is proved in [2], Theorem 5; Remarks (a) and (b) show it to be smoothing of order $[\beta]$. Assertion (i) is proved by noting that

$$\phi H^*\psi-\phi H^{\#}\psi=\sum\phi(T_{nm}a_{nm}{}^*-a_{nm}{}^*T_{nm})\psi.$$

To prove the second assertion, let $\{\phi_i\}$ be a resolution of the identity, with the support of ϕ_i in a coordinate neighborhood U_i with coordinates x^i. Let θ_i have support in U_i, and $\theta_i\equiv 1$ on an open set containing the support of ϕ_i; let ψ_i have support in U_i and $\psi_i\equiv 1$ on an open set containing the support of θ_i. Then

$$T-T_1T_2=\sum_i\psi_i(T-T_1T_2)\phi_i+\sum(1-\psi_i)(T-T_1T_2)\phi_i.$$

Now by Definition 4, $(1-\psi_i)\,T\phi_i$ is completely continuous and smoothing of order $[\beta]$. Also

$$(1-\psi_i)T_1T_2\phi_i=(1-\psi_i)T_1\theta_iT_2\phi_i+(1-\psi_i)T_1(1-\theta_i)T_2\phi_i.$$

Here $(1-\psi_i)T_1\theta_i$ and $(1-\theta_i)T_2\phi_i$ are completely continuous and smoothing of order $[\beta]$ and $T_2\phi_i$ and $(1-\psi_i)T_1$ preserve $L_m{}^p$, $m\leqq[\beta]$; thus $(1-\psi_i)T_1T_2\phi_i$ is completely continuous and smoothing of order $[\beta]$. Now $\psi_i(T-T_1T_2)\phi_i=(\psi_iT\phi_i-\psi_iT_1\theta_iT_2\phi_i)+\psi_iT_1(1-\theta_i)T_2\phi_i$. Here the second term is handled as above, and the first is (modulo completely continuous operators smoothing of order $[\beta]$) $\psi_iH\phi_i-\psi_iH_1\theta_iH_2\phi_i$, where H, H_1 and H_2 are Euclidean $C_\beta{}^\infty$ operators whose symbols, on the image of U_i, are respectively $\sigma(T)$, $\sigma(T_1)$ and $\sigma(T_2)$. They can be extended so that $\sigma(H)=\sigma(H_1)\sigma(H_2)$ and for some R, $\sigma(H_2)(x,z)$ vanishes when $|x|\geqq R$. But $\psi_i(H-H_1\theta_iH_2)\phi_i\equiv\psi_i(H-H_1H_2)\phi_i+\psi_iH_1(1-\theta_i)H_2\phi_i$. For the first term we refer again to Theorem 5 of [2], and the complete continuity of $a(T_{nm}b-bT_{nm})$. In the second term $(1-\theta_i)H_2\phi_i$ is an operator with a bounded kernel in C_β, with bounded support in $E_k\times E_k$. Such an operator is completely continuous and smoothing of order $[\beta]$. This proves Theorem 3.

This shows that, if $\beta\neq 1$, the $C_\beta{}^\infty$ operators form an algebra, and that σ is a homomorphism of this algebra onto the $C_\beta{}^\infty$ functions on $CS(M)$.

THEOREM 4. (Compare [2], Theorem 6). *Let $k>2$ and $\beta\neq 1$. Let M be simply connected; or let $CS(M)$ have a cross-section. Then if $\sigma(T)$ is never zero, there is a $C_\beta{}^\infty$ operator T' which is invertible, and $\sigma(T)=\sigma(T')$.*

Proof. Suppose M is simply connected and $k>2$. Then $CS(M)$ is simply connected, and if $\sigma(T)$ is never zero, we can define $\sigma(T)^{1/n}$ so that $|1-\sigma(T)^{1/n}|<\epsilon$ and the derivatives of order $2k$ of $\sigma(T)^{1/n}$ with respect to cosphere variables are also bounded by ϵ. Then by choosing n large enough, we can, by the comment after Theorem 2, find a $C_\beta{}^\infty$ operator S with symbol $\sigma(T)^{1/n}$ satisfying $\|I-S\|<\frac{1}{2}$. Then S^n is invertible and $\sigma(S^n)=\sigma(T)$.

If $CS(M)$ has a cross-section $\phi\colon M\to CS(M)$, then

$$\{\sigma(T)(p,\phi(p))\}^{-1}\sigma(T)(p,\xi)$$

has an n-th root $G(p,\xi)$ approximating unity as above, so that G is the symbol of an invertible $C_\beta{}^\infty$ operator S. Then $T'=\sigma(T)(p,\phi(p))S^n$ is invertible and $\sigma(T')=\sigma(T)$. This proves Theorem 4.

COROLLARY. *If M and T satisfy the hypotheses of Theorem 4, then the equation $Tf=g$ is equivalent to an equation of the form $f+Kf=g'$, where K is completely continuous.*

D. An example. Let M be a C_∞ Riemannian manifold with metric $r(p,q)$, p and q in M; and let V be a C_β vector field on M. Let $\phi(t)$ be a real function which is identically 1 in a neighborhood of $t=0$, and vanishes outside a larger neighborhood, so that $\phi(r)r^2$ is a C_∞ function on $M\times M$. Let v be the volume element on M associated with the metric r, and let $Kf(p)=H(1,k)^{-1}\int_M\phi(r)r(p,q)^{1-k}f(q)\,dv_q$. Then VK is a $C_\beta{}^\infty$ singular integral operator with symbol $\sigma(VK)(p,\xi)=i\{V(p),\xi/|\xi|\}$, where V is considered as a mapping from M into the tangent bundle, $|\xi|$ is the Riemannian length of the vector ξ in the cotangent bundle, and $\{\ ,\ \}$ indicates the bilinear form relating the tangent and the cotangent bundles. To show this, we need some facts about the metric r.

LEMMA 7. *If $r(x,y)$ is a C_∞ metric on E_k ($r^2(x,y)$ is in C_∞ on E_{2k}), then, for every n and m,*

$$r^m(x,y)=\sum_{i=0}^{n-1}a_i(x,x-y)+R(x,y),$$

where $a_0(x,z)=a_0(x,-z)$, $a_i(x,z)$ is in $C_\infty{}^\infty$ and homogeneous of degree $m+i$; and any derivative of $R(x,y)$ of order $j\leqq n$ is $O(|x-y|^{m+n-j})$.

COROLLARY. $(\partial/\partial x+\partial/\partial y)^\alpha r(x,y)=O(|x-y|)$ *for every* α.

Proof of corollary. In Lemma 7 take $m=1$ and $n=|\alpha|$. Then

$r(x,y)=\sum a_i(x,x-y)+R(x,y)$. If $a_{i\alpha}(x,z)=(\partial/\partial x)^\alpha a_i(x,z)$, then $(\partial/\partial x+\partial/\partial y)^\alpha r(x,y)=\sum_i a_{i\alpha}(x,z)+(\partial/\partial x+\partial/\partial y)^\alpha R(x,y)=O(|x-y|)$.

Proof of the lemma. Let $r^2{}_\alpha(x,y)=(\partial/\partial y)^\alpha r^2(x,y)$. Then

$$\begin{aligned} r^2(x,y) &= \sum_{i=2}^{n+1}\sum_{|\alpha|=i} r^2{}_\alpha(x,x)(y-x)^\alpha/\alpha!+P(x,y)\\ &= \sum_{i=2}^{n+1} b_i(x,x-y)+P(x,y), \end{aligned}$$

where $b_2(x,z)=b_2(x,-z)$, $b_i(x,z)$ is in $C_\infty{}^\infty$ and homogeneous of degree i, and derivatives of P of order $j\leqq n+1$ are $O(|x-y|^{n+2-j})$. Then

$$r^m(x,y)=b_2{}^{m/2}(x,x-y)\{1+\sum_{i=3}^{n+1} b_ib_2{}^{-1}+Pb_2{}^{-1}\}^{m/2}.$$

Using the Taylor expansion for $(1+x)^{m/2}$ with n terms and remainder, we get $r^m(x,y)=\sum a_i(x,x-y)+R(x,y)$, as required in the lemma.

Now let $r^{1-k}(x,y)=\sum_{j=0}^{n-1} a_j(x,x-y)+R(x,y)$, where $n-1=[\beta]$. Then the arguments of Lemmas 2 and 3 and their corollary show that

$$\psi(x)(\partial/\partial x_i)\int \phi(r)a_0(x,x-y)f(y)v(y)\,dy=\psi(x)\int (\partial\phi a_0/\partial x_i)fv\,dy;$$

the multiplication factor $\lim_{\epsilon\to 0}\int_{|x-y|=\epsilon}\phi(r)a_0(x,x-y)\gamma_i\epsilon^{k-1}d\sigma_y$ is absent since a_0 is even on $|x-y|=\epsilon$ and γ_i is odd. In the same way,

$$\|\psi(\partial/\partial x_i)\int \phi(r)a_j(x,x-y)f(y)v(y)\,dy\|_{m+1}\leqq C\|f\|_m$$

for $m<[\beta]$ and $j\geqq 1$. Thus $\psi(\partial/\partial x_i)\int \phi r^{1-k}fv\,dy$ is a $C_\beta{}^\infty$ operator if ψ is in C_β.

It remains to calculate the symbol. Let the coordinates be geodesic at p, so that $a_0(x(p),z)=|z|^{1-k}$, and the kernel of VK is

$$H^{-1}\psi(p)\partial|x-y|^{1-k}/\partial x_i=H(1-k)^{-1}\psi(p)(x_i-y_i)/|x-y|^{k+1}.$$

But it has been shown that the transform of this operator kernel is $(-1)^{\frac{1}{2}}\xi_i/|\xi|$, (see IB), so that the symbol of $\psi(\partial/\partial x_i)K$ is

$$(-1)^{\frac{1}{2}}\psi\xi_i/|\xi|=(-1)^{\frac{1}{2}}\psi\{\partial/\partial x_i,\xi/|\xi|\},$$

using again the fact that the coordinates are normal at p.

A similar argument establishes $V_1 V_2 \int \phi(r) r^{2-k} f \, dv$ as a singular integral operator.

III. Differential Operators and Singular Integral Operators.

Our first goal is to develop a representation of an arbitrary differential operator on $L^p(M)$ in the form of a singular integral operator times a homogeneous differential operator related to the Laplace operator. We begin by discussing the latter operator, using a parametrix as tool. M will be a compact orientable manifold of class C_n $(n \geqq 4)$ and dimension k $(k \geqq 2)$ and with a Riemannian metric $r(p,q)$; $r^2(p,q)$ is a C_{n-1} function for small r.

A. The Laplace operator. Let Δ denote the Laplacian on M. For f in C_2

$$\Delta f = (1/v) \sum (\partial/\partial y_i) v g^{ij} \partial f / \partial y_j,$$

where $v dy_1 \cdots dy_k$ is the volume element in terms of local coordinates, and g_{ij} are components of the metric tensor. Δ is a symmetric operator on its domain C_2, considered as a subspace of $L^2(M, v)$. Let $\bar{\Delta}$ be the closure of Δ as an operator on $L^2(M)$, obtained by closing the graph of Δ in $L^2(M) \times L^2(M)$. f in L^2 is in $D(\bar{\Delta})$, the domain of $\bar{\Delta}$, if there is a sequence $f_n \to f$ such that $f_n \times \Delta f_n \to f \times g$, where $f \times g$ represents an element of $L^2 \times L^2(M)$. It is easy to see that $L_2{}^2(M)$ is in $D(\bar{\Delta})$; for let f be in $L_2{}^2$ and have support in a single coordinate neighborhood (a harmless restriction). Then we can find a sequence of functions f_n in C_2 such that f_n and its derivatives approximate f in $L_2{}^2(E_k)$, hence in $L_2{}^2(M)$. (See, for instance, [2], Lemma 1.) Then both f_n and Δf_n converge in $L^2(M)$.

$\bar{\Delta}$ is symmetric, for $(\bar{\Delta} f, g) = \lim(\Delta f_n, g_n) = \lim(f_n, \Delta g_n) = (f, \bar{\Delta} g)$, where f_n and g_n are in C_2. If d denotes the gradient operator and f is in C_2, then $(\Delta f, f) = -(df, df)$, so for f in C_2 and $\lambda \geqq 0$, $((\lambda - \Delta) f, f) = (df, df) + \lambda(f,f) \geqq \lambda(f,f)$. In particular, all eigenvalues of $\bar{\Delta}$ are non-positive real numbers; for if $\bar{\Delta}\phi = \lambda\phi$, then $\lambda(\phi,\phi) = \lambda(\phi,\phi) + ((\bar{\Delta} - \lambda)\phi, \phi) \leqq 0$. We will show that $\bar{\Delta}$ is self-adjoint, has domain $L_2{}^2(M)$, and has pure point spectrum. The devices used will then be applied to the construction of Λ on the manifold.

Let $\phi(r)$ be identically 1 in $r < \delta$, and vanish for $r > R$. Pick R so that for each p in M the set $\{q : r(p,q) < 2R\}$ is contained in a single C_n coordinate system. Let $\epsilon_\lambda(p,q) = \phi(r(p,q)) E_\lambda(r(p,q))$.

LEMMA 8. *If λ is not a negative real number and f is in $L^2(M)$, then $\epsilon_\lambda f(p) = \int_M \epsilon_\lambda(p,q) f(q)\, dv_q$ is in $L_2^2(M)$.*

Proof. Let f and ψ have support in a single coordinate neighborhood. By Lemma 2 and the estimates (2),

$$(\partial/\partial x_i) \int \psi(x)\phi(r)E_\lambda(r)f(y)v(y)\,dy$$
$$= \int (\partial/\partial x_i)\{\psi(x)\phi(r)E_\lambda(r)\}f(y)v(y)\,dy;$$

and

$$(\partial^2/\partial x_i\partial x_j) \int \psi\phi E_\lambda f\, dv$$
$$= \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial^2/\partial x_i\partial x_j)\{\psi(x)\phi(r)E_\lambda(r)\}f(y)v(y)\,dy$$
$$-\psi(x)f(x)v(x) \lim_{\epsilon\to 0} \int_{|x-y|=\epsilon} (\partial E_\lambda/\partial x_i)\gamma_j\epsilon^{k-1}\, d\sigma_y,$$

if these limits exist as required by Lemma 2. But by (2) and Lemma 7,

$$\partial E_\lambda/\partial x_i = E_\lambda'(r)\partial r/\partial x_i = b_1(x, x-y) + O(|x-y|^{2-k}),$$

and $\partial^2 E_\lambda/\partial x_i\partial x_j = b_0(x, x-y) + O(|x-y|^{1-k})$, where $b_j(x,z)$ $(j=0,1)$ is homogeneous of degree $j-k$ in z, which proves Lemma 8.

LEMMA 9. *If f is in L^2, then*

$$(\bar\Delta - \lambda)\epsilon_\lambda f(p) = f(p) + \int K_\lambda(p,q) f(q)\, dv_q,$$

where $K_\lambda(p,q) = (\Delta-\lambda)_p \epsilon_\lambda(p,q)$ for $p \neq q$. $K_\lambda(p,q)$ is $O(|x-y|^{2-k})$.

Proof. We show first the order of $K_\lambda(p,q)$ by reference to coordinates geodesic at q. In such a system $x(q)=0$, $g_{ij}(0)=\delta_{ij}$, $(\partial g_{ij}/\partial y_k)(0)=0$, $(\partial v/\partial y_k)(0)=0$, and $r^2(p,q) = \sum x_i^2(p)$. Thus

$$\Delta h(x) = h(x)\cdot O(1) + \sum \partial h/\partial x_i \cdot O(|x|) + \sum_{i\neq j} \partial^2 h/\partial x_i\partial x_j \cdot O(|x|^2)$$
$$+ \sum \partial^2 h/\partial x_i^2.$$

Using this with the estimates (2), we see $(\Delta-\lambda)_p\epsilon_\lambda(p,q) = O(|x|^{2-k})$.

Now from the form of the derivatives of $\epsilon_\lambda f(p)$ obtained in the proof of Lemma 8 we get

$$(\bar{\Delta}-\lambda)\epsilon_\lambda f=\lim_{\epsilon\to 0}\int_{|x-y|>\epsilon}\{(\Delta-\lambda)\epsilon_\lambda\}f\,dv$$
$$-f(x)v(x)\sum g^{ij}(x)\lim_{\epsilon\to 0}\int_{|x-y|=\epsilon}(\partial E_\lambda/\partial x_i)\gamma_j\epsilon^{k-1}\,d\sigma_y.$$

By what we have just shown, the $\lim_{\epsilon\to 0}$ on the first integral on the right is superfluous. To evaluate the function which multiplies f, let the coordinates be geodesic at x, so that $v(x)=1$, $g^{ij}(x)=\delta_{ij}$, and

$$\partial E_\lambda(r(x,y))/\partial x_i=\omega_k^{-1}r^{1-k}\partial r/\partial x_i=-\omega_k^{-1}\,|\,x-y\,|^{1-k}\gamma_i.$$

Thus

$$v\sum g^{ij}\lim_{\epsilon\to 0}\int_{|x-y|=\epsilon}(\partial E_\lambda/\partial x_i)\gamma_j\epsilon^{k-1}\,d\sigma_y=-\omega_k^{-1}\int_{|x-y|=\epsilon}\sum\gamma_i^2\,d\sigma_y=-1,$$

which proves the lemma.

Now we show that for $\operatorname{Re}(\lambda)\geqq 0$ and λ sufficiently large, $\bar{\Delta}-\lambda$ has a kernel operator as its inverse. Choose N so that

$$K_\lambda^{(N)}(p,q)=\int\cdots\int K_\lambda(p,p_1)K_\lambda(p_1,p_2)\cdots K_\lambda(p_{N-1},q)\,dv_{p_1}\cdots dv_{p_{N-1}}$$

is bounded. Set

$$F_\lambda(p,q)=\sum_0^{N-1}(-1)^j\int\epsilon_\lambda(p,p_1)K_\lambda^{(j)}(p_1,q)\,dv_{p_1}$$
$$+\int\epsilon_\lambda(p,p_1)f(p_1,q)\,dv_{p_1},\tag{5}$$

where $K_\lambda^{(j)}$ is the j-fold iterate of K_λ. $F_\lambda(p,q)$ is a kernel defining a bounded operator on $L^2(M)$ if $\|f(\cdot,q)\|_2$ is uniformly bounded. In the sense of operators,

$$(\bar{\Delta}-\lambda)F_\lambda=I+(-1)^{N-1}K_\lambda^{(N)}+f+K_\lambda f,$$

where I is the identity, and f the operator with kernel $f(p,q)$. Hence in order for F_λ to be the Green's kernel for $\bar{\Delta}-\lambda$, it is necessary and sufficient that f satisfy

$$(-1)^{N-1}K_\lambda^{(N)}+f+K_\lambda f=0.\tag{6}$$

Now from the estimates (3) and the form of $(\Delta-\lambda)\epsilon_\lambda$ deduced in Lemma 9, a simple integration shows that $|||\,\epsilon_\lambda\,|||\leqq c/|\,\lambda\,|$, and $|||\,K_\lambda\,|||\leqq c/|\,\lambda\,|$, where $|||\,F\,|||$ indicates the sup over $1\leqq r\leqq\infty$ of the norm of the operator with kernel $F(p,q)$ on $L^r(M)$. For on each coordinate neighborhood these operators

are dominated by convolution with a function whose norm in $L^1(E_k)$ is bounded by $c/|\lambda|$. Hence, for $\lambda \geqq L$, $|||K_\lambda||| \leqq \frac{1}{2}$ and

$$F_\lambda = \epsilon_\lambda(1 + \sum_{m=1}^{\infty}(-1)^m K_\lambda^{(m)}), \tag{7}$$

where the series of operators converges in norm, and the series of kernels converges uniformly in the manifold variables and in $\lambda > L$.

PROPOSITION. *The closure of the Laplacian on M is a self-adjoint operator with domain $L_2^2(M)$. It has pure point spectrum, lying on $\lambda \leqq 0$, with a limit only at ∞. The eigenfunction span $L^2(M)$, and the eigenspace of $\lambda = 0$ consists of the constant functions.*

Proof. For f in L^2, $(\bar{\Delta} - L)F_L f = f$; since $\bar{\Delta}$ is symmetric, $F_L^*(\bar{\Delta} - L)g = g$ for g in L_2^2. But for f in L^2, $F_L f$ is in L_2^2, and $F_L f = F_L^*(\bar{\Delta} - L)F_L f = F_L^* f$. Thus F_L is a Hermitian right and left inverse for $\bar{\Delta} - L$; since it is completely continuous, the eigenvalues for $\bar{\Delta} - L$ have a limit only at ∞, and the eigenfunctions span $L^2(M)$. If $\bar{\Delta}\phi = 0$, $0 = (\bar{\Delta}\phi, \phi) = -(d\phi, d\phi)$, so that ϕ has zero (weak) derivatives, from which it can be shown that ϕ is constant. (We do not prove this, nor do we use the fact.) The statement about the domains follows from the fact that range of $F_L \subset L_2^2(M) \subset$ domain of $\bar{\Delta} - L \subset$ range of F_L. The first inclusion is from Lemma 8, the second from a previous remark, and the last from the fact that F_L is the inverse of $\bar{\Delta} - L$.

By assuming one more order of differentiability for M, we could show by this approach that the eigenfunctions of $\bar{\Delta}$ are all in C_2; for by iterating F_L, any function in L^2 can be mapped into C_2.

B. **A semi-group of operators associated with $L - \Delta$.** From now on we will assume M to be a compact orientable C_∞ Riemannian manifold; everything could be done by assuming less, but the frequent statement of differentiability assumptions would be distracting. We denote by Δ the closed self-adjoint operator discussed in the previous section. ϵ_λ, F_λ and K_λ are as above, but L is chosen so that $|||\epsilon_\lambda||| < \frac{1}{2}$ and $|||K_\lambda||| < \frac{1}{2}$ for $|\lambda| \geqq L/2$.

As in the Euclidean case, we can define operators J^α on M by a contour integral:

$$\begin{aligned} J^\alpha = (L - \Delta)^{-\alpha/2} &= \frac{1}{2\pi i}\int_C \lambda^{-\alpha/2}(\lambda - L + \Delta)^{-1} d\lambda \\ &= \frac{1}{2\pi i}\int_C \lambda^{-\alpha/2} F_{L-\lambda} d\lambda, \end{aligned} \tag{8}$$

where C is the path $\operatorname{Re}(\lambda) = L/2$ traversed from top to bottom, and $\lambda^{-\alpha/2}$ is analytic except on $\lambda \leqq 0$. The integrand is a norm-continuous function of λ:

$$(9) \qquad F_{\lambda+h} - F_\lambda = F_\lambda\{(-\lambda + \Delta - h + h)F_{\lambda+h} - I\} = F_\lambda h F_{\lambda+h}.$$

This with the fact that $|||F_\lambda||| = O(1/\lambda)$ shows that the integral converges in operator norm on every $L^p(M)$, $1 \leqq p \leqq \infty$, for $\operatorname{Re}(\lambda) > 0$. Since the Fourier transform is not available to show the properties of this operator, we resort to a Banach algebra approach.

Since $F_\lambda{}^* = F_{\lambda^*}$ and $F_{\lambda_1}F_{\lambda_2} = F_{\lambda_2}F_{\lambda_1}$, the algebra A of operators on $L^2(M)$ generated by the F_λ $(\operatorname{Re}(\lambda) \geqq L/2)$ and I is commutative and self-adjoint, and isometric to its representing function algebra. Let M be a maximal ideal of A, and $\hat{H}(M) = M(H)$ be the representing function of the element H of A. We show that

$$(10) \qquad \hat{J}^\alpha(M) = (-\hat{F}_L(M))^{\alpha/2}.$$

From (9), $\hat{F}_\lambda(M) = 0$ if $\hat{F}_L(M) = 0$, so for these M, (10) holds. Consider $\hat{F}_L(M) \neq 0$. For $-\lambda^{-1}$ not in the spectrum of F_L, $\hat{F}_{L-\lambda}(M) = \hat{F}_L(M)\{1 + \lambda\hat{F}_L(M)\}^{-1}$, by (9). Now

$$\hat{J}^\alpha(M) = \frac{1}{2\pi i}\int_C \lambda^{-\alpha/2}\hat{F}_L(M)\{1 + \lambda\hat{F}_L(M)\}^{-1}\,d\lambda.$$

If we set $\mu = 1/\lambda$, then μ traverses a circle C' counter-clockwise as λ traverses C, and

$$\hat{J}^\alpha(M) = (-\hat{F}_L(M)/2\pi i)\int_{C'} \mu^{(\alpha/2)-1}\{\mu + \hat{F}_L(M)\}^{-1}\,d\mu = \{-\hat{F}_L(M)\}^{\alpha/2},$$

since $-\hat{F}_L(M)$ is inside C'. Thus the J^α form a semi-group of bounded operators on $L^2(M)$ with $J^2 = (L - \Delta)^{-1}$.

C. Further analysis of $J = J^1$, and representation of vector fields. In this section it is shown that $J = J^1$ is a completely continuous operator and smoothing of all orders; and that for any C_β vector field V, VJ is a $C_\beta{}^\infty$ singular integral operator. Finally, the representation of $V_1 \cdots V_n$ as $H(L - \Delta)^{n/2}$, H a singular integral operator, is obtained.

The first step is to change the contour of integration for J to a curve enclosing the negative real axis; this can be justified by considering the representing algebra of A, the separable Banach algebra with identity generated by the F_λ for $\operatorname{Re}(\lambda) \geqq L/2$. Then a change of variables allows us to write

$$J = (\tfrac{1}{\pi}) \int_0^\infty s^{-\frac{1}{2}} F_{L+s}\, ds.$$

That J is completely continuous follows from the fact that this integral can be considered as a strong vector-valued integral in the Banach space generated by the F_λ for $\lambda = L/2$, hence lies in that space of completely continuous operators.

THEOREM 5. *If V is a C_β vector field then VJ is a $C_\beta{}^\infty$ singular integral operator with symbol*

$$\sigma(VJ)(p,\xi) = (-i)\{V, \xi/|\xi|\}.$$

The theorem depends on some facts about the operators ϵ_λ and K_λ. In what follows, $\| \ \|_{m,n}$ indicates the norm of an operator from $L_m{}^p$ to $L_n{}^p$.

i) $\| V\epsilon_\lambda \|_{m,m+1} < A(m)$ $(m \geqq 0)$. A does not depend on λ.

ii) $\| K_\lambda \|_{m,m+1} < B(m)$ $(m \geqq 0)$, B independent of λ.

iii) $\| K_\lambda \|_{m,m} < B(m)/\lambda$ $(m \geqq 0)$, B independent of λ.

Proof of (i). Let $X(t) = 1$ for $t < 1, 0$ for $t > 1$; and $r^{2-k}(x,y) = b(x, x-y) + R(x,y)$, where $b(x,z)$ is the leading term of the expansion in Lemma 7; and let $\partial^2 b(x,z)/\partial x_i \partial x_j = b_{ij}(x,z)$. Then by Lemma 8,

$$(\partial/\partial x_j) \int \psi(\partial\epsilon_\lambda/\partial x_i) f\, dr$$
$$= \lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} (\partial/\partial x_j)(\psi\partial\epsilon_\lambda/\partial x_i) f(y) v(y)\, dy - m(x) f(x),$$

where m is independent of λ. Let $\mu = \lambda^{\frac{1}{2}}$ and dissect the above expression as follows:

$$\lim_{\epsilon\to 0} \int_{|x-y|>\epsilon} X(\mu|x-y|) b_{ij}(x, x-y) f(y) v(y)\, dy$$
$$+ \int X(\mu|x-y|)\{b_{ij}(x,z) - (\partial/\partial x_j)(\psi\partial\epsilon_\lambda/\partial x_i)\} fv\, dy$$
$$+ \int \{1 - X(\mu|x-y|)\}(\partial/\partial x_j)(\psi\partial\epsilon_\lambda/\partial x_i) fv\, dy - m(x) f(x).$$

That the first operator, acting on L^p, has a norm with a bound independent of μ is proved in [1]; the norm of the second is estimated by (2), independently of μ; and the third is treated similarly by (3).

Thus $\| V\epsilon_\lambda \|_{0,1} < C$, where C is independent of λ. To complete the proof of (i), we refer to remarks (b) and (c) and Lemma 2. Let C_α be as in

Remark (c) (*I-D*), $\alpha' = (\alpha_1, \cdots, \alpha_j + 1, \cdots, \alpha_k)$. Then repeated application of Lemma 2 shows that $C_\alpha((\partial/\partial x_j)\psi(\partial/\partial x_i)\epsilon_\lambda - \psi(\partial/\partial x_i)\epsilon_\lambda(\partial/\partial x_j))$ is the operator with kernel $(\partial/\partial x + \partial/\partial y)^{\alpha'}(\psi\partial\phi E_\lambda/\partial x_i)$. But by the Corollary of Lemma 7 and the estimates (3), $|(\partial/\partial x + \partial/\partial y)^{\alpha'}\psi\partial\phi E_\lambda/\partial x_i| < P_n(\mu r)e^{-\mu r}r^{1-k}$ or $< P_n(\mu r)e^{-\mu r}r^{1-k}(\mu r)^{\frac{1}{2}(k-3)}$, so that this operator has a norm which is $O(1/\mu)$. Thus Remarks (b) and (c) show that $\| V\epsilon_\lambda \|_{m,m+1} < A(m)$, with A independent of λ. For (ii), $\| K_\lambda \|_{0,1}$ is found, by direct application of Lemma 2 and the estimates (3), to be $O(\lambda^{-\frac{1}{2}})$, and this is extended to $\| K_\lambda \|_{m,m+1}$ exactly as in (i). (iii) is proved simply by noting that

$$|(\partial/\partial x + \partial/\partial y)^\alpha \phi K_\lambda| < P_n(\mu r)e^{-\mu r}r^{2-k}(\mu r)^{\frac{1}{2}(k-3)} \text{ or } < P_n(\mu r)e^{-\mu r}r^{2-k},$$

and applying Remark (c).

Now to prove the theorem, let $[\beta] = n$ and write

$$\begin{aligned} VJ = (\tfrac{1}{\pi})V\int_0^\infty s^{-\frac{1}{2}}\epsilon_s\,ds - (\tfrac{1}{\pi})V\int_0^L s^{-\frac{1}{2}}\epsilon_s\,ds - (\tfrac{1}{\pi})V\int_0^\infty \{s^{-\frac{1}{2}} - (L+s)^{-\frac{1}{2}}\}\epsilon_{L+s}\,ds \\ \text{(iv)} \qquad + (\tfrac{1}{\pi})\sum_1^n (-1)^m V\int_0^\infty \epsilon_{L+s}K_{L+s}{}^{(m)}s^{-\frac{1}{2}}\,ds \\ + (\tfrac{1}{\pi})V\int_0^\infty \sum_1^\infty (-1)^{n+m}\epsilon_{L+s}K_{L+s}{}^{(n+m)}s^{-\frac{1}{2}}\,ds. \end{aligned}$$

Now from (4) and the definition of ϵ_s,

$$(\tfrac{1}{\pi})\int_0^\infty s^{-\frac{1}{2}}\epsilon_s(r(x,y))\,ds = -H(1,k)^{-1}\phi(r)r^{1-k}.$$

Fubini's theorem shows that $\int_0^\infty s^{-\frac{1}{2}}\epsilon_s\,ds$, considered as an operator integral, is the operator with kernel $\int_0^\infty s^{-\frac{1}{2}}\epsilon_s(r(x,y))\,ds$; thus the first term in (iv) is $-VH(1,k)^{-1}\phi(r)r^{1-k}$, which is the singular integral operator of example II D. In the other terms the differentiation may be carried under the integral and summation since the differentiated integral converges in operator norm:

$$\begin{aligned} &-(\partial g/\partial x_i, \int_0^\infty \sum_1^\infty s^{-\frac{1}{2}}\epsilon_{L+s}K_{L+s}{}^{(m)}\,ds) \\ &= \lim\{-(\partial g/\partial x_i, \sum_1^N \sum_1^M s_n{}^{-\frac{1}{2}}\epsilon_{L+s_n}K_{L+s_n}{}^{(m)}\Delta s_n)\} \\ &= \lim(g, \sum^N \sum^M s_n{}^{-\frac{1}{2}}(\partial/\partial x_i)\epsilon_{L+s_n}K_{L+s_n}{}^{(m)}\Delta s_n) \\ &= (g, \int_0^\infty \sum_1^\infty s^{-\frac{1}{2}}(\partial/\partial x_i)\epsilon_{L+s}K_{L+s}{}^{(m)}\,ds). \end{aligned}$$

Now the second and third terms are bounded from $L_m{}^p$ to $L_{m+1}{}^p$ by (i).

The fourth term is also bounded from L_m^p to L_{m+1}^p by (i) and (iii). In the last term,

$$\| V\epsilon_{L+s}K_{L+s}^{(n+m)} \|_{0,n} \leqq (\| V\epsilon_{L+s}K_{L+s}^{(n-1)} \|_{0,n}) (\| K_{L+s} \|_{0,0}) (\| K_{L+s} \|_{0,0})^m$$
$$\leqq A(n)(c/(L+s))(\tfrac{1}{2})^m,$$

by the choice of L, so that the integrated sum converges to an operator from L^p to L_n^p. This proves Theorem 5.

Since for each vector field V in C_∞, VJ is bounded from L_m^p to L_m^p, J is smoothing of all orders.

LEMMA 10. *If V is a C_β vector field, $VJ-JV$ is smoothing of order $[\beta]$, if $\beta \neq 1$.*

Proof. $J = -H(1,k)^{-1}\phi(r)r^{1-k} + R$. In Theorem 5 it was shown that VR was smoothing of order $[\beta]$. Similarly, RV is smoothing of order $[\beta]$. That the same is true of $VK-KV$, where K is the operator with kernel $\phi(r)r^{1-k}$, is checked with the help of Lemma 7, Lemma 3, and the Corollary of the latter.

Definition 6. For f in L_m^p, $m \geqq 1$, $\Lambda f = (L-\Delta)Jf$.

If f is in L_m^p, $m > 1$, $\Lambda f = J(L-\Delta)f$, since J and $L-\Delta$ commute. It is clear that Λ maps L_m^p into L_{m-1}^p, and that J is its two-sided inverse.

THEOREM 6. *If $\beta \neq 1$ and V_i is a $C_{\beta+i-1}$ vector field, then $V_1 \cdots V_m = H\Lambda^m$, where H is a C_β^∞ singular integral operator with symbol*

$$(-(i))^m \prod_{k=1}^{m} \{V_k, \xi/|\xi|\}.$$

Proof. $$V_1 \cdots V_n = V_1 \cdots V_n J^n \Lambda^n = (V_1J) \cdots (V_nJ)\Lambda^n$$
$$+ \sum_{j=1}^{n-1} V_1 \cdots V_j(V_{j+1}J^j - J^jV_{j+1})JV_{j+2} \cdots JV_n\Lambda^n$$

By Theorem 3 and Theorem 5 $(V_1J) \cdots (V_nJ)$ is a C_β^∞ operator with the prescribed symbol. We show that

$$\sum V_1 \cdots V_j(V_{j+1}J^j - J^jV_{j+1})(JV_{j+2}) \cdots (JV_n)$$

maps L_m^p into L_{m+1}^p by showing that $V_{j+1}J^j - J^jV_{j+1}$ maps L_m^p into L_{m+j}^p. This is done by Lemma 8 and the formula $VJ^j - J^jV = \sum_{k=1}^{j} J^{k-1}(VJ-JV)^{j-k}$. This establishes Theorem 6.

THEOREM 7. *The spaces $L_m{}^p$ $(1 < p < \infty)$ are topologically isomorphic. Any operator on M which is smoothing is also completely continuous.*

Proof. The first statement is proved with the isomorphism J and its inverse Λ. To prove the second, suppose T maps L^p into $L_1{}^p$. Then ΛT is bounded, and $T = J\Lambda T$ is completely continuous.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
HARVEY MUDD COLLEGE.

REFERENCES.

[1] A. P. Calderon and A. Zygmund, "On singular integrals," *American Journal of Mathematics*, vol. 78 (1956), pp. 289-309.

[2] ———, "Singular integral operators and differential equations," *American Journal of Mathematics*, vol. 79 (1957), pp. 901-921.

[3] A. P. Calderon, "Uniqueness in the Cauchy problem for partial differential equations," *American Journal of Mathematics*, vol. 80 (1958), pp. 16-36.

[4] M. P. Gaffney, "The harmonic operator for exterior differential forms," *Proceedings of the American Mathematical Society*, vol. 37 (1951), pp. 48-50.

[5] J. J. Kohn and D. C. Spencer, "Complex Neumann problems," *Annals of Mathematics*, vol. 66 (1957), pp. 89-140.

[6] S. G. Mihlin, "Singular integral equations," *American Mathematical Society Translations*, number 24 (1950).

[7] M. Riesz, "L'integrale de Riemann-Liouville et le probleme de Cauchy," *Acta Mathematica*, vol. 81 (1949), pp. 1-222.

[8] G. N. Watson, *A Treatise on the Theory of Bessel Functions*, Fifth Edition, Cambridge: The University Press, 1952.

CHARACTERIZATIONS OF RIEMANN n-SPHERES.*

By George F. Feeman and Chuan-Chih Hsiung.[1]

Introduction. One of the most interesting classical results in differential geometry in the large is a theorem of Liebmann [14], which states that in ordinary Euclidean space E^3 a closed surface with constant Gaussian curvature is a sphere. For this theorem Hilbert ([8]; or [9], pp. 231-240) gave an ingenious proof, which has since superseded the original one given by Liebmann. It is also well known that in the space E^3 a closed convex surface with constant mean curvature is a sphere. These theorems were extended by Süss [17] to convex hypersurfaces in a Euclidean space E^n of dimension $n \geqq 3$. Recently, Hsiung [10, 11] and Aleksandrov [1, 2] [2] have further extended the results of Süss to hypersurfaces imbedded in a space E^n as well as in an n-dimensional Riemannian manifold of constant Riemannian curvature. In Hsiung's papers the hypersurfaces satisfy a condition weaker than convexity and are so called star-shaped, and in Aleksandrov's the elementary symmetric functions of the principal curvatures of the hypersurfaces are replaced by some more general functions. The purpose of this paper is to use a new method to complete the latter case of Hsiung's work and to further study a more general case in which hypersurfaces are imbedded in a general Riemannian manifold of dimension $\geqq 3$.

In § 1, we first define the vector product of $m-1$ tangent vectors of a Riemannian manifold V^m of dimension $m \geqq 3$ at a point P, and then introduce E. Cartan's system of exterior differential forms for the manifold V^m.

In § 2, from the system of exterior differential forms for the Riemannian manifold V^m introduced in § 1 we geometrically deduce a system for an n-dimensional submanifold V^n of the manifold V^m, where $m > n \geqq 2$. The first and second fundamental forms of the submanifold V^n are obtained, and the generalized covariant differentiation is introduced.

* Received November 28, 1958.

[1] The authors are supported respectively by the Danforth Foundation and the United States Air Force Office of Scientific Research of the Air Research and Development Command, under contract AF 49(638)-215.

[2] The authors are indebted to the referee for calling their attention to the second paper of Aleksandrov.

As a special case of § 1 and § 2, the next section is devoted to the establishment of the fundamental formulas and definitions for a hypersurface V^n imbedded in a Riemannian manifold V^{n+1} of dimension $n+1 \geqq 3$. In particular, the definition of Riemann n-sphere is given, and a differential form concerning a general mean curvature M_α $(\alpha = 1, \cdots, n)$ of the hypersurface V^n is derived by using the combined operator $\otimes$ of the vector product of tangent vectors of the manifold V^{n+1} and the exterior product of differentials (for this operator see, for instance, [12]).

§ 4 contains the statements of two lemmas, which are fundamentally important in the proofs of our main theorems.

Let V^{n+1} be a Riemannian manifold of dimension $n+1 \geqq 3$ and constant Riemannian curvature such that there is a normal coordinate system S of Riemann at a fixed point O covering the whole manifold V^{n+1}. In § 5, we first derive n integral formulas for an orientable hypersurface V^n of class C^3 with boundary V^{n-1} of dimension $n-1$ imbedded in the manifold V^{n+1}, and then for a closed hypersurface V^n to be a Riemann n-sphere we deduce some simple conditions on the mean curvatures M_α $(\alpha = 1, \cdots, n)$ of the hypersurface V^n.

The objective of § 6 is the same as that of § 5, except that in § 6 the Riemannian manifold V^{n+1} is a general one instead of one with constant Riemannian curvature. However, not all results in § 5 are special cases of those in § 6.

1. Riemannian manifolds. Throughout this paper the ranges of indices are given as follows unless stated otherwise:

$$\begin{aligned} &1 \leqq i, j, k, \cdots \leqq m, \\ (1.1) \qquad &1 \leqq \alpha, \beta, \gamma, \cdots \leqq n, \\ &n+1 \leqq A, B, C, \cdots \leqq m \qquad (m > n). \end{aligned}$$

We shall also follow the usual tensor convention that when the same letter appears in any term as a subscript and superscript, it is understood that this letter is summed for all the possible values.

Let V^m be a Riemannian manifold of dimension $m \geqq 3$ and class C^3, y^i a set of local coordinates of a point P on the manifold V^m, and $a_{ij}dy^i dy^j$ the fundamental form of the manifold V^m, where $a_{ij} = a_{ji}$ and the matrix (a_{ij}) is positive definite so that the determinant $| a_{ij} | = a$ is positive.

Now let A_r $(r = 1, \cdots, m-1)$ be $m-1$ tangent vectors of the manifold V^m at the point P, and let A_r^i $(r = 1, \cdots, m-1)$ be the contravariant com-

ponents of the vector A_r in the local coordinates $y^1, \cdots, y^m$ of the point P. Let $A_1 \times \cdots \times A_{m-1}$ denote the vector product of the $m-1$ vectors $A_1, \cdots, A_{m-1}$, which is defined to be the tangent of the manifold V^m at the point P whose j-th contravariant component is (see, for instance, Hsiung [11])

$$(1.2)\quad (A_1 \times \cdots \times A_{m-1})^j = (-1)^{m-1} a^{-\frac{1}{2}} \begin{vmatrix} \delta_1{}^j & \delta_2{}^j & \cdots & \delta_m{}^j \\ a_{i1}A_1{}^i & a_{i2}A_1{}^i & \cdots & a_{im}A_1{}^i \\ \cdot & \cdot & \cdot & \cdot \\ a_{i1}A_{m-1}{}^i & a_{i2}A_{m-1}{}^i & \cdots & a_{im}A_{m-1}{}^i \end{vmatrix},$$

where $\delta_i{}^j$ are the Kronecker deltas.[8] Let I be a tangent vector of the manifold V^m at the point P with contravariant components I^i in $y^1, \cdots, y^m$. From the definition of the scalar product of any two vectors, A_r and A_s, namely,

$$(1.3)\quad A_r \cdot A_s = a_{ij} A_r{}^i A_s{}^j,$$

it follows that the scalar product of the two vectors I and $A_1 \times \cdots \times A_{m-1}$ is given by

$$(1.4)\quad I \cdot A_1 \times \cdots \times A_{m-1} = (-1)^{m-1} a^{\frac{1}{2}} \,|\, I, A_1, \cdots, A_{m-1} \,|,$$

where $|\, I, A_1, \cdots, A_{m-1} \,|$ is a determinant, the elements of each of whose columns are the contravariant components of the vector indicated. Thus from equation (1.4) it follows immediately that the vector $A_1 \times \cdots \times A_{m-1}$ is orthogonal to each of the $m-1$ vectors $A_1, \cdots A_{m-1}$.

Now consider a frame $Pe_1 \cdots e_m$, where $e_1, \cdots, e_m$ form an ordered set of m mutually orthogonal unit tangent vectors of the manifold V^m at a point P so that

$$(1.5)\quad e_i \cdot e_j = a_{hk} e_i{}^h e_j{}^k = \delta_{ij},$$

where δ_{ij} are the Kronecker deltas. The position vector Y of the point P is defined to be the tangent vector of the manifold V^m at the point P whose contravariant components are the local coordinates $y^1, \cdots, y^m$ of the point P. Then we can write

$$(1.6)\quad dY = \omega^i e_i,$$

$$(1.7)\quad de_i = \omega_i{}^j e_j,$$

where d denotes the exterior differentiation, and ω^i, $\omega_i{}^j$ are Pfaffian forms in the y's satisfying

$$(1.8)\quad \omega_i{}^j + \omega_j{}^i = 0.$$

[8] The authors wish to thank Professor E. H. Cutler for some discussions about the form of the formula (1.2).

$$R_{\alpha\beta\gamma\delta}=(\Omega_{\alpha\gamma}\Omega_{\beta\delta}-\Omega_{\alpha\delta}\Omega_{\beta\gamma})+\bar{R}_{hijk}y^h{}_{,\alpha}y^i{}_{,\beta}y^j{}_{,\gamma}y^k{}_{,\delta}, \tag{3.20}$$

$$\Omega_{\alpha\beta,\gamma}-\Omega_{\alpha\gamma,\beta}=-\bar{R}_{hijk}e_{n+1}{}^h y^i{}_{,\alpha}y^j{}_{,\beta}y^k{}_{,\gamma}, \tag{3.21}$$

where $R_{\alpha\beta\gamma\delta}$ and $\bar{R}_{hijk}$ are Riemann symbols formed with the tensors $g_{\alpha\beta}$ and a_{ij} respectively.

In particular, if the manifold V^{n+1} is of constant Riemannian curvature K, from the definition of the Riemannian curvature K it follows that

$$\bar{R}_{hijk}=K(a_{hj}a_{ik}-a_{hk}a_{ij}), \tag{3.22}$$

and therefore equations (3.20) and (3.21) can be reduced to

$$R_{\alpha\beta\gamma\delta}=(\Omega_{\alpha\gamma}\Omega_{\beta\delta}-\Omega_{\alpha\delta}\Omega_{\beta\gamma})+K(g_{\alpha\gamma}g_{\beta\delta}-g_{\alpha\delta}g_{\beta\gamma}), \tag{3.23}$$

$$\Omega_{\alpha\beta,\gamma}-\Omega_{\alpha\gamma,\beta}=0. \tag{3.24}$$

Furthermore, substitution of equations (3.15), (3.20) and (3.24) in equation (3.19) and use of $\Omega_{\alpha\beta}=\Omega_{\beta\alpha}$ give immediately

$$e_{n+1\,;\alpha\beta}-e_{n+1\,;\beta\alpha}=\psi_{\alpha\beta}e_{n+1}, \tag{3.25}$$

where

$$\psi_{\alpha\beta}=g^{\gamma\delta}(R_{\beta\alpha\gamma\delta}-\bar{R}_{hijk}y^h{}_{,\beta}y^i{}_{,\alpha}y^j{}_{,\gamma}y^k{}_{,\delta})=0. \tag{3.26}$$

Thus we obtain

$$d^2e_{n+1}=\tfrac{1}{2}\psi_{\alpha\beta}(dx^\beta\wedge dx^\alpha)e_{n+1}=0. \tag{3.27}$$

From equations (2.6) and (2.7) it is easily seen that the n principal curvatures $k_1,\cdots,k_n$ of the hypersurface V^n at a point P are roots of the determinant equation

$$|\,b_{\alpha\beta}-k\delta_{\alpha\beta}\,|=0. \tag{3.28}$$

In other words, $k_1,\cdots,k_n$ are the characteristic roots of the matrix $(b_{\alpha\beta})$. The α-th mean curvature M_α of the hypersurface V^n at the point P is defined by

$$C_\alpha{}^n M_\alpha=S_\alpha \qquad (\alpha=1,\cdots,n), \tag{3.29}$$

where S_α is the α-th elementary symmetric function of $k_1,\cdots,k_n$, and $C_\alpha{}^n$ is a binomial coefficient.

A principal minor of the matrix $(b_{\alpha\beta})$ is a minor whose diagonal is a part of the main diagonal of the matrix $(b_{\alpha\beta})$. From a theorem in linear algebra (see, for instance, [16], Chapter VII) it is known that the α-th elementary symmetric function of the characteristic roots of the matrix $(b_{\alpha\beta})$ is equal to the sum of all α-rowed principal minors of the matrix $(b_{\alpha\beta})$.

Therefore $C_\alpha{}^n M_\alpha$ is equal to the sum of all α-rowed principal minors of the matrix $(b_{\alpha\beta})$. In particular, we have

$$nM_1 = \sum_{\alpha=1}^{n} b_{\alpha\alpha}, \tag{3.30}$$

$$M_n = |\, b_{\alpha\beta}\,| = b, \tag{3.31}$$

$$nM_{n-1} = \sum_{\alpha=1}^{n} B^{\alpha\alpha}, \tag{3.32}$$

where $B^{\alpha\alpha}$ is the cofactor of $b_{\alpha\alpha}$ in the determinant b.

We shall introduce the combined operator $\otimes$ of the vector product $\times$ and the exterior product $\wedge$, as defined in the paper [12] for the case where the manifold V^{n+1} is a Euclidean space.

Let $A^1,\cdots,A^n$ be n tangent vectors of the manifold V^{n+1} at a point P, and suppose that the components of each vector A^α $(\alpha=1,\cdots,n)$ in the local coordinates $y^1,\cdots,y^{n+1}$ of the point P are differentiable functions of the n variables $x^1,\cdots,x^n$. Combining the vector product of vectors and the exterior product of differentials, we can define the vector

$$\begin{aligned} &A^1\otimes\cdots\otimes A^j\otimes dA^{j+1}\otimes\cdots\otimes dA^n \\ &= (A^1\times\cdots\times A^j\times A^{j+1}{}_{;i_{j+1}}\times\cdots\times A^n{}_{;i_n})\,dx^{i_{j+1}}\wedge\cdots\wedge dx^{i_n}, \\ &\qquad (j=1,\cdots,n). \end{aligned} \tag{3.33}$$

It is obvious that the vector (3.33) is independent of the order of the vectors $dA^{j+1},\cdots,dA^n$.

From equations (1.6), (2.3), (3.2), (3.12) and (3.14) it is easy to obtain

$$\underbrace{dY\otimes\cdots\otimes dY}_{n} = n!(\omega^1\wedge\cdots\wedge\omega^n)\,e_{n+1}, \tag{3.34}$$

$$\begin{aligned} \underbrace{dY\otimes\cdots\otimes dY}_{n} &= Y_{,\alpha_1}dx^{\alpha_1}\otimes\cdots\otimes Y_{,\alpha_n}dx^{\alpha_n} \\ &= n!(Y_{,1}\times\cdots\times Y_{,n})\,dx^1\wedge\cdots\wedge dx^n \\ &= n!\,e_{n+1}dA. \end{aligned} \tag{3.35}$$

Comparison of equation (3.34) with equation (3.35) yields immediately

$$dA = \omega^1\wedge\cdots\wedge\omega^n. \tag{3.36}$$

Similarly, by means of equations (1.6), (1.7), (1.8), (2.3) and (2.5), we have

$$\underbrace{dY\otimes\cdots\otimes dY}_{n-\alpha}\otimes\underbrace{de_{n+1}\otimes\cdots\otimes de_{n+1}}_{\alpha}$$
$$=(-1)^{\alpha}(n-\alpha)!\,\alpha!\sum_{\substack{\beta_1<\cdots<\beta_{n-\alpha}\\ \beta_{n-\alpha+1}<\cdots<\beta_n}}(\omega^{\beta_1}e_{\beta_1}\otimes\cdots\otimes\omega^{\beta_{n-\alpha}}e_{\beta_{n-\alpha}}$$
$$\otimes\, b_{\beta_{n-\alpha+1},\gamma_1}\omega^{\gamma_1}e_{\beta_{n-\alpha+1}}\otimes\cdots\otimes b_{\beta_n,\gamma_\alpha}\omega^{\gamma_\alpha}e_{\beta_n}).$$

It is easily seen that in the last expression we need only to consider the terms, for which $\gamma_1,\cdots,\gamma_\alpha$ take the values $\beta_{n-\alpha+1},\cdots,\beta_n$, and therefore the subscripts of the b's will contain none of the values $\beta_1,\cdots,\beta_{n-\alpha}$; as all other terms are zero. Making use of equations (3.12), (3.36) and the elementary identity $C_\alpha^n=n!/[(n-\alpha)!\alpha!]$, we thus obtain

$$\underbrace{dY\otimes\cdots\otimes dY}_{n-\alpha}\otimes\underbrace{de_{n+1}\otimes\cdots\otimes de_{n+1}}_{\alpha}\tag{3.37}$$
$$=(-1)^{\alpha}(n-\alpha)!\,\alpha!(e_1\times\cdots\times e_n)(\omega^1\wedge\cdots\wedge\omega^n)$$
$$[\text{sum of all }\alpha\text{-rowed principal minors of the matrix }(b_{\alpha\beta})]$$
$$=(-1)^{\alpha}n!\,M_\alpha e_{n+1}\,dA.$$

A closed hypersurface V^n in a Riemannian manifold V^{n+1} of dimension $n+1\geqq 3$ is called a Riemann n-sphere if every point of the hypersurface V^n is umbilical. Concerning umbilical points the following lemma is well known.

LEMMA 3.1. *A point P of a hypersurface V^n imbedded in a Riemannian manifold V^{n+1} of dimension $n+1\geqq 3$ is umbilical if $k_1=\cdots=k_n$ at the point P.*

Proof. It is well known that the principal curvatures $k_1,\cdots,k_n$ of the hypersurface V^n at the point P are the extremal values of the quantity k defined by

$$k=(\Omega_{\alpha\beta}q^\alpha q^\beta)/(g_{\alpha\beta}q^\alpha q^\beta)$$

at the point P for an arbitrary tangent vector q of the hypersurface V^n with contravariant components q^α. Thus the assumption that $k_1=\cdots=k_n$ at the point P implies that the quantity k is independent of the vector q, so that $\Omega_{\alpha\beta}=cg_{\alpha\beta}$ for all α and β at the point P, where c is a scalar invariant. Hence the point P of the hypersurface V^n is umbilical (see, for instance, [5], p. 179).

Now consider, for example,[4] a three-dimensional Riemannian space V^3 with the fundamental form

[4] The authors are indebted to the referee for suggesting this example.

$$ds^2 = (\sum_{i=1}^{3} y_i^2)^c \sum_{j=1}^{3} dy_j^2,$$

where c is a constant $\geqq 2$. A straightforward calculation shows that the space V^3, excluding the origin $(0,0,0)$, is not of constant curvature and that every point of the surface in the space V^3 given by the parametric equations

$$y^1 = \sin x^1 \cos x^2, \qquad y^2 = \sin x^1 \sin x^2, \qquad y^3 = \cos x^1$$

is umbilical.

4. Lemmas. In this section we shall state two lemmas, which will be needed for later development. The proofs of the lemmas will be omitted here, but can be found in [7], pp. 52, 104, 105.

LEMMA 4.1. *Let S_r be the r-th elementary symmetric function of n real nonzero numbers $k_1, \cdots k_n$, and suppose that $M_0 = 1$ and $M_r = S_r/C_r^n$ for $r = 1, \cdots, n$. Then*

$$M_{r-1}M_{r+1} - M_r^2 \leqq 0 \qquad (r = 1, \cdots, n-1), \tag{4.1}$$

where the equality for any value of r implies that $k_1 = \cdots = k_n$.

LEMMA 4.2. *Let $k_1, \cdots, k_n$, M_0 and M_r be defined as in Lemma 4.1. If $M_1, \cdots, M_s$, $1 \leqq s \leqq n$, are positive, then*

$$M_1 \geqq M_2^{\frac{1}{2}} \geqq M_3^{1/3} \geqq \cdots \geqq M_s^{1/s} \qquad (1 \leqq s \leqq n), \tag{4.2}$$

where the equality at any stage implies that $k_1 = \cdots = k_n$.

5. Riemann n-spheres on Riemannian manifolds of constant curvature. Let O be a point on a Riemannian manifold V^{n+1} of dimension $n+1$, and U a sufficiently small neighborhood of the point O on the manifold V^{n+1} such that in the neighborhood U there exists a unique geodesic ρ joining the point O to every point P of the neighborhood U. Let $g_1, \cdots, g_{n+1}$ be $n+1$ mutually orthogonal geodesics of the manifold V^{n+1} through the point O. Then the normal coordinates $y^1, \cdots, y^{n+1}$ of Riemann of the point P with respect to the geodesic frame $Og_1 \cdots g_{n+1}$ are defined by $y^i = s\cos(\rho, g_i)$, where (ρ, g_i) is the angle between the geodesic ρ and the geodesic g_i at the point O, and s is the arc length from the point O to the point P along the geodesic ρ. It is obvious that $\sum_{i=1}^{n+1} \cos^2(\rho, g_i) = 1$. If on the manifold V^{n+1} there exists a unique geodesic arc with minimal length joining a fixed point

O to every point P, then we can have a normal coördinate system of Riemann at the fixed point O covering the whole manifold V^{n+1}.

THEOREM 5.1. *Let V^{n+1} be a Riemannian manifold of dimension $n+1 \geqq 3$ and constant Riemannian curvature K such that there is a normal coordinate system S of Riemann at a fixed point O covering the whole manifold V^{n+1}. Then for a closed orientable hypersurface V^n of class C^3 imbedded in the manifold V^{n+1}*

$$\int_{V^n} M_{\alpha-1}\, dA + \int_{V^n} M_\alpha p\, dA = 0 \qquad (\alpha = 1, \cdots, n), \tag{5.1}$$

where $|M_1|$ is sufficiently large at least at some points of the hypersurface V^n, and p is the scalar product of the unit normal vector e_{n+1} of the hypersurface V^n at a point P and the position vector Y of the point P with respect to the coordinate system S.

Proof. We first consider an orientable hypersurface V^n of class C^3 with boundary V^{n-1} of dimension $n-1 \geqq 1$ imbedded in the Riemannian manifold V^{n+1}, and shall use the results of the preceding sections with the same notations except that here Y is the position vector of a point P on the hypersurface V^n with respect to the fixed normal coordinate system S of Riemann.

Applying the ordinary rules for differentiation of determinants and recalling that a can be regarded as a constant in generalized covariant differentiation, we obtain the differential form

$$\begin{aligned}
(5.2)\quad & d[(-1)^n a^{\frac{1}{2}} | \underbrace{dY, \cdots, dY}_{n-\alpha}, Y, e_{n+1}, \underbrace{de_{n+1}, \cdots, de_{n+1}}_{\alpha-1} |] \\
&= \sum_{\beta=1}^{n-\alpha} [(-1)^n a^{\frac{1}{2}} | \underbrace{\overbrace{dY, \cdots, dY}^{\beta-1}, d^2Y, dY, \cdots, dY}_{n-\alpha}, Y, e_{n+1}, \underbrace{de_{n+1}, \cdots, de_{n+1}}_{\alpha-1} |] \\
&\qquad + (-1)^{\alpha-1} a^{\frac{1}{2}} | e_{n+1}, \underbrace{dY, \cdots, dY}_{n-\alpha+1}, \underbrace{de_{n+1}, \cdots, de_{n+1}}_{\alpha-1} | \\
&\qquad + (-1)^{\alpha} a^{\frac{1}{2}} | Y, \underbrace{dY, \cdots, dY}_{n-\alpha}, \underbrace{de_{n+1}, \cdots, de_{n+1}}_{\alpha} | \\
&+ \sum_{\beta=1}^{\alpha-1} [(-1)^n a^{\frac{1}{2}} | \underbrace{dY, \cdots, dY}_{n-\alpha}, Y, e_{n+1}, \underbrace{\overbrace{de_{n+1}, \cdots, de_{n+1}}^{\beta-1}, d^2e_{n+1}, de_{n+1}, \cdots, de_{n+1}}_{\alpha-1} |],
\end{aligned}$$

where $\alpha = 1, \cdots, n$. By means of the equation $d^2Y = 0$ mentioned in § 1

and equation (3.27), it follows immediately that the first and fourth members on the right side of equation (5.2) vanish. We thus obtain, in consequence of equations (1.4) and (3.37),

$$(5.3)\quad d[(-1)^n a^{\frac{1}{2}} \mid \underbrace{dY,\cdots,dY}_{n-\alpha}, Y, e_{n+1}, \underbrace{de_{n+1},\cdots,de_{n+1}}_{\alpha-1} \mid]$$

$$= (-1)^{n-\alpha+1} e_{n+1}\cdot(\underbrace{dY\otimes\cdots\otimes dY}_{n-\alpha+1} \otimes \underbrace{de_{n+1}\otimes\cdots\otimes de_{n+1}}_{\alpha-1})$$

$$+ (-1)^{n-\alpha} Y\cdot(\underbrace{dY\otimes\cdots\otimes dY}_{n-\alpha} \otimes \underbrace{de_{n+1}\otimes\cdots\otimes de_{n+1}}_{\alpha})$$

$$= (-1)^n n!(M_{\alpha-1}\, dA + M_\alpha p\, dA),$$

where $p = Y\cdot e_{n+1}$. Integrating equation (5.3) over the hypersurface V^n and applying Stokes' Theorem to the left side of the equation, we arrive at the integral formulas

$$(5.4)\quad \int_{V^n} M_{\alpha-1}\, dA + \int_{V^n} M_\alpha p\, dA$$

$$= (1/n!) \int_{V^{n-1}} a^{\frac{1}{2}} \mid \underbrace{dY,\cdots,dY}_{n-\alpha}, Y, e_{n+1}, \underbrace{de_{n+1},\cdots,de_{n+1}}_{\alpha-1} \mid,$$

$$(\alpha = 1,\cdots,n).$$

In particular, when V^n is closed, the right side of equation (5.4) vanishes, and hence we have the formulas (5.1).

THEOREM 5.2. *Let V^n $(n \geqq 2)$ be a hypersurface on a Riemannian manifold V^{n+1} satisfying the conditions of Theorem 5.1. Suppose that there exists an integer s, $1 \leqq s \leqq n-1$, such that $M_s > 0$, and either $p \leqq -M_{s-1}/M_s$ or $p \geqq -M_{s-1}/M_s$ at all points of the hypersurface V^n. Then V^n is a Riemann n-sphere.*

Proof. Since $M_s > 0$, the conditions $p \leqq -M_{s-1}/M_s$ and $p \geqq -M_{s-1}/M_s$ are respectively equivalent to $M_s p + M_{s-1} \leqq 0$ and $M_s p + M_{s-1} \geqq 0$. Equation (5.1) for $\alpha = s$, together with either of these two inequalities, implies that $p = -M_{s-1}/M_s$. Substituting this value of p in equation (5.1) for $\alpha = s+1$, we obtain

$$(5.5)\quad \int_{V^n} (1/M_s)(M_s{}^2 - M_{s-1}M_{s+1})\, dA = 0.$$

Due to the inequality (4.1) for $r = s$, the integrand on the left side of equation

(5.5) is nonnegative, and therefore equation (5.5) holds when and only when

$$M_s^2 - M_{s-1}M_{s+1} = 0. \tag{5.6}$$

From Lemma 4.1 it follows immediately that $k_1 = \cdots = k_n$ at all points of the hyersurface V^n, and by Lemma 3.1 we thus prove Theorem 5.2.

THEOREM 5.3. *Let V^n $(n \geqq 2)$ be a hypersurface on a Riemannian manifold V^{n+1} satisfying the conditions of Theorem 5.1. Suppose that there exists an integer s, $1 \leqq s \leqq n$, such that at all points of the hypersurface V^n the function p is of the same sign, $M_i > 0$ for $i = 1, \cdots, s$, and M_s is constant. Then the hypersurface V^n is a Riemann n-sphere.*

Proof. *Case* 1. $s < n$. By the inequalities (4.1) for $r = 1, \cdots, s$ and the assumption that $M_i > 0$ for $i = 1, \cdots, s$, we obtain

$$M_1/M_0 \geqq M_2/M_1 \geqq \cdots \geqq M_{s+1}/M_s,$$

and in particular

$$M_1 M_s \geqq M_{s+1}, \tag{5.7}$$

where the equality implies that $k_1 = \cdots = k_n$. From equation (5.1) for $\alpha = 1$ and the assumptions that $M_1 > 0$ and p is of the same sign at all points of the hypersurface V^n, it follows that p must be negative. Multiplying both sides of the inequality (5.7) by p, integrating over the hypersurface V^n, and applying equation (5.1) for $\alpha = 1$ and $\alpha = s + 1$, we can readily obtain, in consequence of the assumption that M_s is constant,

$$-M_s \int_{V^n} dA = \int_{V^n} M_1 M_s p \, dA \leqq \int_{V^n} M_{s+1} p \, dA = -M_s \int_{V^n} dA,$$

from which it follows that

$$\int_{V^n} (M_1 M_s - M_{s+1}) p \, dA = 0. \tag{5.8}$$

Due to the inequality (5.7) the integrand on the left side of equation (5.8) is nonpositive, and therefore $M_1 M_s - M_{s-1} = 0$. From Lemma 4.1 it follows that $k_1 = \cdots = k_n$ at all points of the hypersurface V^n, and by Lemma 3.1 Theorem 5.3 for $s < n$ is therefore proved.

Case 2. $s = n$. By using the assumption that $M_i > 0$ for $i = 1, \cdots, n$, from Lemma 4.2 we have the inequalities

$$M_1 \geqq M_2^{1/2} \geqq \cdots \geqq M_{n-1}^{1/(n-1)} \geqq M_n^{1/n} = c, \tag{5.9}$$

where c is a positive constant. By means of equation (5.1) for $\alpha = n$ and

the inequalities (5.9) we obtain

$$(5.10) \qquad \int_{V^n} M_n p\, dA = -\int_{V^n} M_{n-1}\, dA \leqq -c^{n-1} \int_{V^n} dA.$$

On the other hand, making use of equation (5.1) for $\alpha = 1$, the inequalities (5.9) and the fact that $p < 0$, we have

$$(5.11) \qquad \int_{V^n} M_n p\, dA = c^{n-1} \int_{V^n} M_n^{1/n} p\, dA$$
$$\geqq c^{n-1} \int_{V^n} M_1 p\, dA = -c^{n-1} \int_{V^n} dA.$$

Combination of (5.10) and (5.11) yields immediately

$$(5.12) \qquad \int_{V^n} (M_n^{1/n} - M_1) p\, dA = 0.$$

Due to the inequalities (5.9), the integrand on the left side of equation (5.12) is nonnegative, and therefore $M_n^{1/n} = M_1$, which by Lemma 4.2 implies that $k_1 = \cdots = k_n$ at all points of the hypersurface V^n. Hence the proof of Theorem 5.3 is complete by Lemma 3.1.

In the case where V^{n+1} is a Euclidean space and V^n is a convex hypersurface of class C^2 instead of C^3; the formulas (5.1) were obtained by Minkowski [15] for $n = 2$ and by Kubota [13] for a general n, Theorem 5.2 with further restrictions that $s = 1$ and the equality holds in the last conditions was obtained by Grotemeyer [6] for $n = 2$ and by Süss [18] for a general n, and Theorem 5.3 was obtained by Liebmann [14] for $n = 2$ and by Süss [17] for a general n.

By using different methods, Hsiung [11, 10] obtained the formulas (5.1) for $\alpha = 1, n$ and some special cases of Theorems 5.2 and 5.3; and also the formulas (5.1) for $\alpha = 1, \cdots, n$, together with Theorems 5.2 and 5.3, in the case where V^{n+1} is a Euclidean space and the hypersurface V^n is of class C^2 instead of C^3. The proofs of Theorems 5.2 and 5.3 here are essentially the same as those given by Hsiung in the second paper just mentioned.

6. Riemann n-spheres on Riemannian manifolds of dimension $n + 1 \geqq 4$.

THEOREM 6.1. *Let V^{n+1} be a Riemannian manifold of dimension $n + 1 \geqq 3$ such that there is a normal coordinate system S of Riemann at a fixed point O covering the whole manifold V^{n+1}. Then for a closed orientable hypersurface V^n of class C^3 imbedded in the manifold V^{n+1}*

$$(6.1) \qquad \int_{V^n} M_{\alpha-1}\, dA + \int_{V^n} M_\alpha p\, dA = 0,$$

where $|M_1|$ *is sufficiently large at least at some points of the hypersurface* V^n, α *is an odd integer less than or equal to* n, *and* p *is defined as in Theorem* 5.1.

Proof. The proof of Theorem 6.1 is exactly the same as that of Theorem 5.1, except that this time α is an odd integer and the vanishing of the fourth member on the right side of equation (5.2) is due to the pairwise cancellation of its terms.

By using a different method, Hsiung [11] obtained the formula (6.1) for $\alpha = 1$ in the case where the hypersurface V^n is of class C^2 instead of C^3.

THEOREM 6.2. *Let* V^n $(n \geqq 3)$ *be a hypersurface on a Riemannian manifold* V^{n+1} *satisfying the conditions of Theorem* 6.1. *Suppose that there exists an odd integer* s, $1 < s \leqq n$, *such that* $M_i > 0$ *for* $i = s, s-1, s-2$, *and either* $p \leqq -M_{s-1}/M_s$ *or* $p \geqq -M_{s-1}/M_s$ *at all points of the hypersurface* V^n. *Then* V^n *is a Riemann* n*-sphere.*

Proof. By the same argument as in the proof of Theorem 5.2, equation (6.1) for $\alpha = s$, together with either of the two inequalities $M_s p + M_{s-1} \leqq 0$ and $M_s p + M_{s-1} \geqq 0$, implies that $p = -M_{s-1}/M_s$. Substituting this value of p in equation (6.1) for $\alpha = s-2$, which is an odd integer by assumption, we obtain

$$(6.2) \qquad \int_{V^n} (1/M_s)\,(M_{s-3}M_s - M_{s-2}M_{s-1})\, dA = 0.$$

Since M_{s-1} and M_{s-2} are positive, from inequalities (4.1) for $r = s-1$ and $r = s-2$, we obtain

$$(6.3) \qquad M_{s-3}/M_{s-2} \leqq M_{s-2}/M_{s-1} \leqq M_{s-1}/M_s,$$

from which it follows that $M_{s-3}M_s - M_{s-2}M_{s-1} \leqq 0$. Thus the integrand on the left side of equation (6.2) is nonpositive, and the equality in (6.3) holds. From Lemma 4.1 it follows immediately that $k_1 = \cdots = k_n$ at all points of the hypersurface V^n, and by Lemma 3.1 Theorem 6.2 is therefore proved.

THEOREM 6.3. *Let* V^n $(n \geqq 3)$ *be a hypersurface on a Riemannian manifold* V^{n+1} *satisfying the conditions of Theorem* 6.1. *Suppose that there exists an odd integer* s, $1 < s \leqq n$, *such that at all points of the hypersurface* V^n *the function* p *is of the same sign,* $M_i > 0$ *for* $i = 1, \cdots, s-1$, *and either* M_{s-1} *or* M_s *is constant. Then* V^n *is a Riemann* n*-sphere.*

Proof. *Case* 1. M_{s-1} is constant. Multiplying both sides of equation (6.1) for $\alpha=1$ by M_{s-1} and subtracting the resulting equation from equation (6.1) for $\alpha=s$, we obtain

$$(6.4)\qquad \int_{V^n}(M_s-M_1M_{s-1})p\,dA=0.$$

Since $M_1, M_2, \cdots, M_{s-1}$ are assumed to be positive, the inequalities (4.1) for $r=1,\cdots,s-1$ can be written together as

$$(6.5)\qquad M_1\geqq M_2/M_1\geqq M_3/M_2\geqq\cdots\geqq M_s/M_{s-1},$$

from which it follows immediately that $M_s-M_1M_{s-1}\leqq 0$. On the other hand, by using equation (6.1) for $\alpha=1$ and the assumptions that $M_1>0$ and p is of the same sign at all points of the hypersurface V^n, it is easily seen that p is negative. Thus the integrand on the left side of equation (6.4) is nonnegative, and the equality in (6.5) holds. From Lemma 4.1 it follows immediately that $k_1=\cdots=k_n$ at all points of the hypersurface V^n, and therefore by Lemma 3.1 V^n is a Riemann n-sphere.

Case 2. M_s is constant. Since s is an odd integer and $M_i>0$ for $i=1,\cdots,s-1$, from Lemma 4.2 we have the inequalities

$$(6.6)\qquad M_1\geqq M_2^{1/2}\geqq\cdots\geqq M_{s-1}^{1/(s-1)}\geqq M_s^{1/s}=c,$$

where c is a constant. By means of equation (6.1) for $\alpha=s$ and the inequalities (6.6) we obtain

$$(6.7)\qquad \int_{V^n}M_sp\,dA=-\int_{V^n}M_{s-1}dA\leqq -c^{s-1}\int_{V^n}dA.$$

On the other hand, making use of equation (6.1) for $\alpha=1$, the inequalities (6.6) and the fact that $p<0$, we have

$$(6.8)\qquad \int_{V^n}M_sp\,dA=c^{s-1}\int_{V^n}M_s^{1/s}p\,dA$$
$$\geqq c^{s-1}\int_{V^n}M_1p\,dA=-c^{s-1}\int_{V^n}dA.$$

Combination of (6.7) and (6.8) yields immediately

$$(6.9)\qquad \int_{V^n}(M_s^{1/s}-M_1)p\,dA=0.$$

Due to the inequalities (6.6), the integrand on the left side of equation (6.9) is nonnegative, and therefore $M_s^{1/s}=M_1$, which by Lemma 4.2 implies that

$k_1 = \cdots = k_n$ at all points of the hypersurface V^n. Using Lemma 3.1 we therefore complete the proof of Theorem 6.3.

MUHLENBERG COLLEGE
AND
LEHIGH UNIVERSITY.

REFERENCES.

[1] A. D. Aleksandrov, "Uniqueness theorems for surfaces in the large. I," (in Russian), *Vestnik Leningradskogo Univerciteta*, vol. 11, no. 19 (1956), pp. 5-17.

[2] ———, "Uniqueness theorems for surfaces in the large. V," (in Russian), *Vestnik Leningradskogo Universiteta*, vol. 13, no. 19 (1958), pp. 5-8.

[3] E. Cartan, *Les Systèmes Différentiels Extérieurs et Leurs Applications Géométrique*, Paris, 1945.

[4] ———, *Leçons sur la Géométrie des Espaces de Riemann*, Paris, 1951.

[5] L. P. Eisenhart, *Riemannian Geometry*, Princeton, 1949.

[6] K.-P. Grotemeyer, "Eine kennzeichnende Eigenschaft der Affinsphären," *Archiv der Mathematik*, vol. 3 (1952), pp. 307-310.

[7] G. H. Hardy, J. E. Littlewood, G. Pólya, *Inequalities*, Cambridge, 1934.

[8] D. Hilbert, "Über Flächen von konstanter Gaussscher Krümmung," *Transactions of the American Mathematical Society*, vol. 2 (1901), pp. 87-99.

[9] ———, *Grundlagen der Geometrie*, 7th edition, Leipzig and Berlin, 1930.

[10] C. C. Hsiung, "Some integral formulas for closed hypersurfaces," *Mathematica Scandinavica*, vol. 2 (1954), pp. 286-294.

[11] ———, "Some integral formulas for closed hypersurfaces in Riemannian space," *Pacific Journal of Mathematics*, vol. 6 (1956), pp. 291-299.

[12] ———, "Some global theorems on hypersurfaces," *Canadian Journal of Mathematics*, vol. 9 (1957), pp. 5-14.

[13] T. Kubota, "Über konvexgeschlossene Mannigfaltigkeiten im n-dimensionalen Raume," *Science Reports of the Tôhoku Imperial University*, ser. 1, vol. 14 (1925), pp. 85-99.

[14] H. Liebmann, "Eine neue Eigenschaft der Kugel," *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, (1899), pp. 44-55.

[15] H. Minkowski, "Volumen und Oberfläche," *Mathematische Annalen*, vol. 57 (1903), pp. 447-495.

[16] L. Mirsky, *An Introduction to Linear Algebra*, Oxford, 1955.

[17] W. Süss, "Zur relativen Differentialgeometrie. V.: Über Eihyperflächen im R^{n+1}," *Tôhoku Mathematical Journal*, vol. 31 (1929), pp. 202-209.

[18] ———, "Über Kennzeichnungen der Kugeln und Affinsphären durch Herrn K.-P. Grotemeyer," *Archiv der Mathematik*, vol. 3 (1952), pp. 311-313.

[19] A. W. Tucker, "On generalised covariant differentiation," *Annals of Mathematics*, vol. 32 (1931), pp. 451-460.

REPRESENTATIONS FOR COMPLETELY CONVEX FUNCTIONS.*

By R. P. Boas, Jr.

1. Introduction. Let $f(x)$ be a completely convex function on $[0,1]$, that is, an infinitely differentiable function such that $(-1)^n f^{(2n)}(x) \geqq 0$. Such a function is necesarily the restriction to $[0,1]$ of an entire function of exponential type π [1], [3], [4], [5]. The most familiar completely convex function is $\sin \pi x$. Wintner [6] recently established another necessary condition for completely convex functions: if f is completely convex on $[0,1]$, it can be written in the form $f(x) = q(\cos \pi x)$, where $q(z) = (1-z^2)^{\frac{1}{2}} p(z)$, $p(z) = \sum_{r=0}^{\infty} \mu_r z^r$, $\mu_r = \int_{-1}^{1} u^r \, d\alpha(u)$, and $\alpha(u)$ is nondecreasing. However, this condition is not sufficient: as Wintner pointed out, the simplest choices of α (except $\alpha(u) = \operatorname{sgn} u$) fail to lead to completely convex f.

I shall obtain a necessary and sufficient condition for an f of Wintner's form to be completely convex. In the light of this condition, it is not surprising that simple choices of α fail to generate completely convex functions, since it turns out that α must be, except for a possible jump at 0, absolutely continuous, with a derivative $F(u)$ of the form

$$\phi\{\tfrac{1}{\pi}\log[u^{-1}(-1+(1-u^2)^{\frac{1}{2}})]\}(1-u^2)^{-\frac{1}{2}}, \qquad u < 0;$$

$$\psi\{\tfrac{1}{\pi}\log[u^{-1}(1+(1-u^2)^{\frac{1}{2}})]\}(1-u^2)^{-\frac{1}{2}}, \qquad u > 0,$$

where $\phi(t)$ and $\psi(t)$ are themselves entire functions, of the form

$$\sum_{n=0}^{\infty} a_n t^{2n}/(2n)!$$

with $a_n \geqq 0$ and $\sum \pi^{-2n} a_n$ convergent. A perhaps simpler characterization of completely convex functions on $[0,1]$ is by means of the integral representation

$$(1) \qquad f(x) = \sin \pi x \cdot \{c + \int_0^{\infty} (\cosh \pi t + \cos \pi x)^{-1} \phi(t)\, dt + \int_0^{\infty} (\cosh \pi t - \cos \pi x)^{-1} \psi(t)\, dt\},$$

where $c \geqq 0$ and ϕ and ψ are as specified in the preceding sentence.

I am indebted to D. V. Widder for helpful discussions.

* Received December 4, 1958.

2. The integral representation. If $f(x)$ is completely convex in $[0,1]$, there is a largest number c such that $f(x) - c\sin \pi x$ is also completely convex function $g(x)$. Then $f(x) = c \sin \pi x + g(x)$, and $g(x)$ is a minimal completely convex function; that is, $g(x)$ is completely convex, and no function $g(x) - c \sin \pi x$, $c > 0$, is completely convex. The results of the present paper depend on the following known characterization [4] of minimal completely convex functions by their expansions in Lidstone series: $f(x)$ is a minimal completely convex function on $[0,1]$ if and only if

$$f(x) = \sum_{n=0}^{\infty} \{a_n \Lambda_n(x) + b_n \Lambda_n(1-x)\}, \tag{2}$$

where $(-1)^n a_n \geqq 0$, $(-1)^n b_n \geqq 0$ (in fact, $a_n = f^{(2n)}(1)$, $b_n = f^{(2n)}(0)$), and $\Lambda_n(x)$ is the polynomial of degree n which for $0 < x < 1$ has the Fourier series

$$\Lambda_n(x) = 2\pi^{-2n-1}(-1)^n \sum_{k=1}^{\infty} (-1)^{k+1} k^{-2n-1} \sin k\pi x. \tag{3}$$

Suppose that f has the representation (2); it is known that the series converges for all complex values of x, uniformly on compact sets. Since we have [2]

$$-i(-1)^n \Lambda_n(iy) \geqq \tfrac{2}{3} y \pi^{-2n} \tag{4}$$

and since $(-1)^n f^{(2n)}(1) \geqq 0$, the convergence of the first part of (2) implies that

$$\sum | f^{(2n)}(1) | \pi^{-2n} \quad \text{converges} \tag{5}$$

and hence, since $f(1-x)$ is a minimal completely convex function with $f(x)$, that $\sum | f^{(2n)}(0) | \pi^{-2n}$ converges.

Using the Fourier series (3), we now have, for $0 < x < 1$,

$$\begin{aligned} f(x) &= 2 \sum_{n=0}^{\infty} (-1)^n f^{(2n)}(1) \pi^{-2n-1} \sum_{k=1}^{\infty} (-1)^{k+1} k^{-2n-1} \sin k\pi x \\ &\qquad + 2 \sum_{n=0}^{\infty} (-1)^n f^{(2n)}(0) \pi^{-2n-1} \sum_{k=1}^{\infty} k^{-2n-1} \sin k\pi x \\ &= 2\Im\{ \sum_{n=0}^{\infty} (-1)^n f^{(2n)}(1) \sum_{k=1}^{\infty} (-1)^{k+1} (k\pi)^{-2n-1} e^{ik\pi x} \\ &\qquad + \sum_{n=0}^{\infty} (-1)^n f^{(2n)}(0) \sum_{k=1}^{\infty} (k\pi)^{-2n-1} e^{ik\pi x} \} \\ &= 2\Im\{ \sum_{n=0}^{\infty} (-1)^n f^{(2n)}(1)/(2n)! \sum_{k=1}^{\infty} (-1)^{k+1} e^{ik\pi x} \int_0^{\infty} e^{-k\pi t} t^{2n}\, dt \\ &\qquad + \sum_{n=0}^{\infty} (-1)^n f^{(2n)}(0)/(2n)! \sum_{k=1}^{\infty} e^{ik\pi x} \int_0^{\infty} e^{-k\pi t} t^{2n}\, dt \}. \end{aligned} \tag{6}$$

Now

$$\sum_{k=1}^{\infty}\int_0^{\infty} e^{-k\pi t}t^{2n}\,dt=\sum_{k=1}^{\infty}(2n)\,!\,(k\pi)^{-2n-1}$$

converges for $n>0$, so for $n>0$ the integrals in (6) can be taken outside the sums over k. For $n=0$, we have by direct computation

$$\sum_{k=1}^{\infty} e^{ik\pi x}\int_0^{\infty} e^{-k\pi t}\,dt=\sum_{k=1}^{\infty}(k\pi)^{-1}e^{ik\pi x}=-\pi^{-1}\log(1-e^{i\pi x})$$

and

$$\int_0^{\infty} dt\sum_{k=1}^{\infty} e^{ik\pi x-k\pi t}=\int_0^{\infty}(e^{\pi t-i\pi x}-1)^{-1}\,dt=-\pi^{-1}\log(1-e^{i\pi x}),$$

so that the change of order of operations is also legitimate for $n=0$. Hence we have

$$f(x)=2\Im\{\sum_{n=0}^{\infty}(-1)^n f^{(2n)}(1)/(2n)\,!\int_0^{\infty} t^{2n}\sum_{k=1}^{\infty}(-1)^{k+1}e^{ik\pi x-k\pi t}\,dt$$
$$+\sum_{n=0}^{\infty}(-1)^n f^{(2n)}(0)/(2n)\,!\int_0^{\infty} t^{2n}\sum_{k=1}^{\infty} e^{ik\pi x-k\pi t}\,dt\},$$

$$f(x)=2\Im\{\sum_{n=0}^{\infty}(-1)^n f^{(2)n}(1)/(2n)\,!\int_0^{\infty} t^{2n}[e^{-\pi(ix-t)}+1]^{-1}\,dt$$
$$+\sum_{n=0}^{\infty}(-1)^n f^{(2n)}(0)/(2n)\,!\int_0^{\infty} t^{2n}[e^{-\pi(ix-t)}-1]^{-1}\,dt\}. \tag{7}$$

Now

$$\sum_{n=0}^{\infty}|f^{(2n)}(1)|/(2n)\,!\int_0^{\infty} e^{-\pi t}t^{2n}\,dt$$

converges by (5). Since $|e^{-\pi(ix-t)}+1|\geqq e^{\pi t}-1$,

$$\sum_{n=0}^{\infty}|f^{(2n)}(1)|/(2n)\,!\int_1^{\infty} t^{2n}\,|e^{-\pi(ix-t)}+1|^{-1}\,dt$$

converges; and

$$\sum_{n=0}^{\infty}|f^{(2n)}(1)|/(2n)\,!\int_0^{1} t^{2n}\,|e^{-\pi(ix-t)}+1|^{-1}\,dt$$

converges (for fixed x) since the integrand is bounded. Thus in the first sum in (7) we can change the order of summation and integration, and similar considerations apply to the second sum. Put

$$\phi(t)=\sum_{n=0}^{\infty}(-1)^n f^{(2n)}(1)t^{2n}/(2n)\,!=\tfrac{1}{2}[f(1+it)+f(1-it)],$$

$$\psi(t)=\sum_{n=0}^{\infty}(-1)^n f^{(2n)}(0)t^{2n}/(2n)\,!=\tfrac{1}{2}[f(it)+f(-it)].$$

Then from (7) we obtain

$$f(x)=2\Im\{\int_0^\infty \phi(t)\,[e^{-\pi(ix-t)}+1]^{-1}\,dt+\int_0^\infty \psi(t)\,[e^{-\pi(ix-t)}-1]^{-1}\,dt\},$$

$$(8)\quad f(x)=\sin\pi x\cdot\{\int_0^\infty \phi(t)\,[\cosh\pi t+\cos\pi x]^{-1}\,dt + \int_0^\infty \psi(t)\,[\cosh\pi t-\cos\pi x]^{-1}\,dt\}$$

(which we may recognize as the representation of $f(x)$ by the Poisson integral for the strip $0<x<1$). Thus every minimal completely convex function has the representation (8).

Conversely, if functions $\phi(t)$ and $\psi(t)$ are defined by

$$(9)\qquad \phi(t)=\sum_{n=0}^{\infty} a_n t^{2n}/(2n)\,!,\qquad \psi(t)=\sum_{n=0}^{\infty} b_n t^{2n}/(2n)\,!,$$

with $a_n\geqq 0$, $b_n\geqq 0$, and $\sum \pi^{-2n}a_n$, $\sum \pi^{-2n}b_n$ convergent, and we define $f(x)$ by (8) for $0<x<1$, all our steps are reversible and lead to

$$f(x)=\sum_{n=0}^{\infty}\{(-1)^n a_n\Lambda_n(x)+(-1)^n b_n\Lambda_n(1-x)\},$$

which is known to imply [4] that $f(x)$ is a minimal completely convex function.

Since every completely convex function differs from a minimal one by $c\sin\pi x$, we have proved the following theorem.

THEOREM. *A function f defined on $0\leqq x\leqq 1$ is completely convex if and only if it has the form*

$$(10)\qquad f(x)=\sin\pi x\cdot\{c+\int_0^\infty \phi(t)\,[\cosh\pi t+\cos\pi x]^{-1}\,dt + \int_0^\infty \psi(t)\,[\cosh\pi t-\cos\pi t]^{-1}\,dt\},$$

where $c\geqq 0$, and ϕ and ψ are even entire functions of exponential type π with nonnegative Maclaurin coefficients.

3. Wintner's representation. The representation (10) can be transformed as follows. Expand $\cosh\pi t+\cos\pi x$ in powers of $(\cos\pi x)/\cosh\pi t$, obtaining

$$f(x)=\sin\pi x\cdot\{\int_0^\infty \phi(t)\,dt\sum_{r=0}^{\infty}(-1)^r\cos^r\pi x(\cosh\pi t)^{-r-1} + \int_0^\infty \psi(t)\,dt\sum_{r=0}^{\infty}\cos^r\pi x(\cosh\pi t)^{-r-1}\}.$$

Since $\phi(t)$ and $\psi(t)$ are $O(e^{\pi t})$, the two integrals are dominated by

$$\sum_{r=0}^{\infty} |\cos^r \pi x| \int_0^{\infty} e^{-\pi r t}\, dt = \sum_{r=0}^{\infty} (\pi r)^{-1} |\cos^r \pi x|,$$

which converges for $0 < x < 1$. Hence we have

$$f(x) = \sin \pi x \cdot \{ \sum_{r=0}^{\infty} (-1)^r \cos^r \pi x \int_0^{\infty} \phi(t) (\cosh \pi t)^{-r-1}\, dt$$
$$+ \sum_{r=0}^{\infty} \cos^r \pi x \int_0^{\infty} \psi(t) (\cosh \pi t)^{-r-1}\, dt\}.$$

In the first integral put $\cosh \pi t = -u^{-1}$, in the second put $\cosh \pi t = u^{-1}$; we obtain

$$f(x) = \pi^{-1} \sin \pi x \cdot \{ \sum_{r=0}^{\infty} \cos^r \pi x \int_{-1}^{0} \phi\{\tfrac{1}{\pi} \cosh^{-1}(-1/u)\} u^r (1-u^2)^{-\frac{1}{2}}\, du$$
$$+ \sum_{r=0}^{\infty} \cos^r \pi x \int_0^1 \psi\{\tfrac{1}{\pi} \cosh^{-1}(1/u)\} u^r (1-u^2)^{-\frac{1}{2}}\, du$$
$$= \sin \pi x \cdot \sum_{r=0}^{\infty} \cos^r \pi x \int_{-1}^{1} u^r F(u)\, du,$$

where (in particular) $F(u) \geqq 0$. Thus if we put

$$\mu_r = \int_{-1}^{1} u^r F(u)\, du, \tag{11}$$
$$p(z) = \sum_{r=0}^{\infty} \mu_r z^r,$$
$$q(z) = (1-z^2)^{\frac{1}{2}} p(z),$$

we have $f(x) = q(\cos \pi x)$, which is Wintner's result. However, we have not only this necessary condition, but also the necessary and sufficient condition that f has this form, where

$$F(u) = \phi\{\tfrac{1}{\pi} \cosh^{-1}(-1/u)\} (1-u\ )^{-\frac{1}{2}}, \qquad u < 0,$$
$$F(u) = \psi\{\tfrac{1}{\pi} \cosh^{-1}(1/u)\} (1-u^2)^{-\frac{1}{2}}, \qquad u > 0,$$

with ϕ and ψ as in (9). To include completely convex functions that are not minimal, we have only to replace $F(u)\,du$ in (11) by $d\alpha(u)$, where $\alpha(u) = \int_{-1}^{u} F(t)\, dt + c \operatorname{sgn} u.$

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] S. Bernstein, "Remarks on the theory of regularly montonic functions," *Izvestiya Akademiya Nauk SSSR*, Seriya Matematicheskaia, vol. 16 (1952), pp. 3-16 = *Sobranie Sochinenii*, vol. 2, Akademiya Nauk SSSR,, 1954, pp. 546-559.

[2] R. P. Boas, Jr., "Representation of functions by Lidstone series," *Duke Mathematical Journal*, vol. 10 (1943), pp. 239-245.

[3] D. V. Widder, "Functions whose even derivatives have a prescribed sign," *Proceedings of the National Academy of Sciences*, U. S. A., vol. 26 (1940), pp. 657-659.

[4] ———, "Completely convex functions and Lidstone series," *Transactions of the American Mathmatical Society*, vol. 51 (1942), pp. 387-398.

[5] ———, *The Laplace transform*, Princeton, 1941.

[6] A. Wintner, "On cosine-like arches," *American Journal of Mathematics*, vol. 80 (1958), pp. 125-130.

EIGENFUNCTION EXPANSIONS FOR NON-SYMMETRIC PARTIAL DIFFERENTIAL OPERATORS, III.*

By Felix E. Browder.[1]

In two previous papers under the same title ([7], [8]), the writer has constructed a theory of eigenfunction expansions of a generalized Plancherel-Weyl type for general classes of realizations of a partial differential operator L on an open subset G of E^n, the subnormal realizations in [7] and the decomposable realizations in [8]. These results were established without any restrictions upon G, the type of L, or on the smoothness or behaviour of the coefficients of L at the boundary of G or at infinity. Results of the same type were obtained for expansions in solutions of the equations $(L-\zeta B)u=0$ for positive differential operators B.

It is the purpose of the present paper to extend and generalize these results in two separate directions. In the first place, it is very difficult to determine in any concrete case whether a particular realization of a partial differential operator under specific boundary conditions falls within either of the two classes which we have studied, except in the relatively simple case in which L is symmetric. For this reason, we have begun the study elsewhere ([5], [6], [9]) of the simplest of the basically non-symmetric cases, elliptic operators on unbounded domains under Dirichlet boundary conditions, but the results obtained at this level of generality do not as yet permit us to apply the theory as previously constructed. On the other hand, for the regular case on a bounded domain, the completeness of the eigenfunctions of the Dirichlet problem was proved by the writer in [4] by a method which extends to the whole class of regular variational boundary-value problems. It is of interest, therefore, to obtain some results on the completeness of the eigenfunctions of L for L singular but elliptic, without any assumption on the boundedness or smoothness in the large of its coefficients. In section 1, we show that if f is a distribution with compact support in G and if L satisfies certain simple local conditions at each point of G, then the orthogonality of f to each eigenfunction

* Received December 29, 1958.

[1] This paper was written while the writer held a National Science Foundation Senior Post-Doctoral Fellowship.

of arbitrary order of L on G implies that $f=0$. The equivalent and somewhat more intuitive dual form of this result is that the eigenfunctions of L are complete in $C^\infty(G)$. The proof combines a refinement of the author's results in [4] with the Runge theorem for solutions of elliptic equations due to Lax [14] and Malgrange [15].

In section 2, we are concerned with another sort of extension of the eigenfunction expansion theory, the generalization of Bochner's theorem to eigenfunction expansions. Next to the Plancherel theory, the theorem of Bochner-Herglotz, which asserts that a continuous function on R^1 is positive definite if and only if it is the Fourier-Stieltjes transform of a positive finite measure, is probably the most often-applied result of classical Fourier analysis, and it is not surprising that its extension to the domain of eigenfunction expansions has attracted interest. (We remark that the proof of the Bochner theorem generalized in a rather different way to a Banach algebra context is presented in [16].) A generalization of Bochner's theorem to eigenfunction expansions for ordinary differential operators was given by M. Krein [13] in 1946, whose results also contained as a special case Bernstein's theorem on the representation of completely monotonic functions as Laplace-Stieltjes transforms of positive measures ([17], p. 160). More recently, Berezanski ([3], [4]) has given a proof of a similar theorem for elliptic differential operators from which the Bochner and Bernstein theorems follow as special cases. If L is a linear elliptic differential operator with smooth complex-valued coefficients on an open subset G of E^n, L' its formal adjoint, $\bar{L}$ the differential operator on G whose coefficients are the complex conjugates of those of L, a function $\psi(x,y,\lambda)$ on $G\times G\times R^1$ is said to be an elementary kernel for L on G if for each fixed λ in R^1, ψ is positive definite on $G\times G$ and of class C^m in x and y separately while $L_x\psi=\bar{L}_y\psi=\lambda\psi$. In terms of the notion of elementary kernel, Berezanski's theorem asserts that if $K(x,y)$ is a continuous positive-definite function on $G\times G$, then $K(x,y)$ has a representation of the form

$$K(x,y)=\int_{R^1}\psi(x,y,\lambda)\,dm(\lambda) \tag{1}$$

for some elementary kernel ψ and a positive finite measure m on R^1 if and only if

$$\int_{G\times G}K(x,y)\bar{f}(x)\,(L'g)\,(y)\,dx\,dy = \int_{G\times G}K(x,y)\,(\overline{L'f})\,(x)\,g(y)\,dx\,dy, \tag{2}$$

for every pair of functions f and g in $C_0^\infty(G)$, the family of infinitely differ-

entiable functions with compact support in G. In addition, he shows in [3] that $\psi(x,y,\lambda)$ may be written in the form $\sum_j \phi_j(x,\lambda)\bar{\phi}_j(y,\lambda)$, where $(L-\lambda I)\phi_j=0$. In section 2 below, using a different procedure from [2] and [3], we shall establish a similar theorem for the case when L is not necessarily elliptic. The eigenfunctions which we obtain (and the elementary kernel, as well) are not, except in the hypoelliptic case, differentiable functions, but in contrast with the results for the Plancherel theory, they are locally integrable functions which are weak eigenfunctions and not distributions. We also obtain a similar representation theorem under more general hypotheses in terms of eigenfunctions with complex eigenvalues.

1. Throughout this and the following section, we shall employ the notation of [8].

Let $L=\sum_{|\alpha|\leqq 2m} a_\alpha(x)D^\alpha$ be a partial differential operator of order $2m$ $(m\geqq 1)$, on an open subset G of the Euclidean n-space E^n. We shall suppose for the sake of simplicity that the coefficients of L are infinite differentiable at each point of G, although the arguments which we put forward may be carried through under rather mild local regularity assumptions, as the perceptive reader will observe. We recall that L is elliptic at x if the $2m$-form $h(x,\xi)=\sum_{|\alpha|=2m} a_\alpha(x)\xi^\alpha>0$ for all real n-vectors $\xi\neq 0$. $(\xi^\alpha=(\xi_1)^{\alpha_1}\cdots(\xi_n)^{\alpha_n}.)$

In the present section, our basic assumptions on L are ellipticity at each point of G and uniqueness of the solution of the Cauchy problem in the small for $(L'-\zeta)$, where ζ is any complex number and L' is the adjoint differential operator to L, defined by $L'u=\sum_{|\alpha|\leqq 2m}(-1)^{|\alpha|}D^\alpha(\bar{a}_\alpha(x)u)$. To be precise, the second assumption may be formulated as follows: (U. C. P. S.): If G_0 is a connected open subset of G, ζ a complex number, and u a function in $C^\infty(G_0)$ such that $(L'-\zeta)u=0$, and if u is identically zero on an open subset of G_0, then u is identically zero throughout G_0.

It follows from a classical argument of Holmgren (and also from the theorem that solutions of linear elliptic equations with analytic coefficients are analytic) that if L has coefficients which are real analytic functions in G, then (U. C. P. S.) holds. A more general result in the same direction follows from the recent work of Calderon [10], who has shown that if the characteristic form $h(x,\xi)$ of L' has simple characteristic roots in the complex domain with respect to every direction, then (U. C. P. S.) holds. In particular, this assumption is valid for all second-order equations. (For the bibliography of the earlier work of Muller, Heinz, Hartman and Wintner, and Aronszajn on

the second-order case, we refer to [10].) In the case of two independent variables, the result was obtained for all elliptic equations with similar restrictions on characteristic roots by Carleman. The theorems due to Carleman and Calderon are valid under very mild differentiability assumptions on the coefficients, and therefore a fortiori under our present assumption.

Under the assumption (U. C. P. S.) (restricted to $\zeta = 0$), Lax [14] and Malgrange [15] have established the following generalization of Runge's theorem for solutions of elliptic equations: Suppose the uniqueness of the solution of the Cauchy problem in the small for the elliptic operator L' and let G_0 be an open subset of G such that $G - G_0$ has no compact components in G. Then if u is a solution of $Lu = 0$ in G_0 and K is a precompact open subset of G_0, u may be approximated in $C^\infty(K)$ by a solution v of $Lv = 0$ in G. (Theorem 6, p. 341 of [15].)

The eigenfunctions of our partial differential operator L on G are defined as the solutions for some $s > 0$ and some complex ζ of the equation $(L - \zeta)^s u = 0$. Since we are assuming that the coefficients of L are infinitely differentiable and that L, and hence $(L - \zeta)^s$, is elliptic, we may restrict our attention to eigenfunctions lying in $C^\infty(G)$. The order of an eigenfunction u is the least positive s for which there exists a complex ζ with $(L - \zeta I)^s u = 0$. From the Lax-Malgrange generalization of the Runge theorem, we deduce the following result which will be useful in the proof of the main theorem of this section:

LEMMA 1. *Let L be a linear elliptic differential operator on G with infinitely differentiable coefficients for which (U.C.P.S.) holds, G_0 an open subset of G such that $G - G_0$ has no compact components in G, K a precompact open subset of G_0. If u is an eigenfunction of order s of L with eigenvalue ζ on G_0, then u may be approximated with arbitrary closeness in $C^\infty(K)$ by eigenfunctions v of L of order $\leqq s$ and eigenvalue ζ on the larger domain G.*

Proof. Since $(L - \zeta)^s$ is an elliptic differential operator, it suffices by the Runge theorem to show that if w is a solution of the equation $((L - \zeta)^s)' w = 0$ in a connected open subset G_1 of G, and if w vanishes on an open subset of G_1, then w vanishes identically on G_1. We remark first that $((L - \zeta)^s)' = (L' - \bar{\zeta})^s$. Let $w_1 = (L' - \bar{\zeta})^{s-1} w$. Then w_1 is a solution of $(L - \bar{\zeta}) w_1 = 0$ in G_1 which vanishes on an open subset of the connected open set G_1. By the assumption (U. C. P. S.), w_1 must vanish everywhere on G_1, i.e., $(L' - \bar{\zeta})^{s-1} w = 0$ in G_1. Proceeding by induction, it follows that $w = 0$, and the proof is complete.

LEMMA 2. *Let G be an open subset of E^n, K a precompact subset of G. Then there exists a pre-compact open subset G_0 of G which contains K for which $G - G_0$ has no compact components.*

Proof of Lemma 2. We may assume K compact. Let $\epsilon > 0$ be less than the positive distance from the compact set K to $E^n - G$. For each x in K, let $B_\epsilon(x) = \{y : d(x,y) < \epsilon\}$. By compactness, K may be covered by a finite family $\{B_1, \cdots, B_k\}$ of these ϵ-disks, each of which is contained in G, together with its closure. Let $G_0' = \bigcup_k B_k$. G_0' is a pre-compact open subset of G. Let $\{C_j\}$ be the family of compact components of $G - G_0'$. Each C_j is compact and open in $G - G_0'$. (To verify the last fact, we need only show that $G - G_0'$ is locally connected. But $G - \mathrm{cl}(G_0')$ being an open subset of E^n is locally connected, and a sufficiently small neighborhood in $G - G_0'$ of a point on the boundary of G_0' is identical with a neighborhood of that point in $E^n - G_0'$, and the latter is locally connected.) Since $G - G_0'$ is open in $E^n - G_0'$, each C_j is open in $E^n - G_0'$, and hence, being compact, connected, and open in $E^n - G_0'$, must be a component of $E^n - G_0'$. But the latter set has only a finite number of components, so that there are only finitely many C_j and the distance from any C_j to the non-compact components of $G - G_0'$ has a positive lower bound ϵ_1. If we set $G_0 = G_0' \cup \bigcup_j C_j$, then $G - G_0$ has no compact components and, since G_0 is bounded and its ϵ_2-neighborhood is contained in G for $\epsilon_2 = \min(\epsilon, \epsilon_1)$, G_0 is a pre-compact subset of G which contains K.

If G_0 is a pre-compact subset of G, the coefficients of our differential operator L have all their derivatives continuous and uniformly bounded on G_0. If we consider the Dirichlet problem in the variational sense on G_0, as in [4], for the elliptic operator L, it will be regular in the sense that if (ϕ, ψ) is the inner product in $L^2(G_0)$, there exist $c_0 > 0$, $k \geqq 0$ such that for all ϕ in $C_c^\infty(G_0)$, $(-1)^m \operatorname{Re}(L\phi, \phi) + k(\phi, \phi) \geqq c_0 \sum_{|\beta| \leqq m} (D^\beta \phi, D^\beta \phi)$. It follows that the generalized Friedrichs extension of the operator $(L + (-1)^m kI)$ with domain $C_c^\infty(G_0)$ has a compact inverse R defined on the whole of $L^2(G_0)$.

Let $A_{2m} = \sum_{|\beta| \leqq m} (-1)^{|\beta|} D^\beta D^\beta$. Using the Fourier transform of tempered distributions, one may construct an elementary solution $e_{2m}(x - y)$ for A_{2m} on $L^2(E^n)$ which lies in C^∞ off the diagonal and such that, if B is any disk containing the closure of G_0 in its interior and $\epsilon > 0$, then for x and y in B, $| e_{2m}(x - y) | \leqq K_\epsilon \{ | x - y |^{2m-n-\epsilon} + 1 \}$. It follows by a standard argument that there exists a C^∞ function $r(x, y)$ on $G \times G$, such that if u is a distribution solution of the equation $A_{2m} u = f$ for an integrable function on B, then

$u(x) = \int_B e_{2m}(x-y)f(y)\,dy + \int_B r(x,y)u(y)\,dy$, for almost all x in G_0. If R_2 is a bounded linear mapping of $L^2(G_0)$ into itself such that $A_m Rf = f$, then on G_0, $(Rf)(x) = E(f)(x)$, where E is the integral operator with kernel $e_{2m}(x-y) + (R_2^*)_y r(x,y)$. If P is the projection mapping of $L^2(B)$ on $L^2(G_0)$ obtained by restriction, it follows that for $2mj > n/2$, $(PR_2P)^j = (PEP)^j$ is an operator of Hilbert-Schmidt type.

THEOREM 1. *The eigenfunctions of the Dirichlet problem for L (i.e., for the generalized Friedrichs extension of L restricted to $C_c^\infty(G_0)$) on the relatively compact open subset G_0 of G are complete in $L^2(G_0)$ and in $C^\infty(G_0)$ in their respective topologies.*

Proof of Theorem 1. Completeness in $L^2(G_0)$ will follow from the proof of Theorem 1 of [4] and the following lemma:

LEMMA 3. *For sufficiently large j, more specifically $2mj > n/2$, R^j is an operator of Hilbert-Schmidt type.*

Proof of Lemma 3. It follows from the argument of [4] that $R = SR_1$, where S is a bounded operator in $L^2(G_0)$ and R_1 in the inverse of $(L_s + (-1)^m kI)$, with L_s the Friedrichs extension of the symmetric part of L, taken as a semi-bounded operator with domain $C_c^\infty(G_0)$. It suffices to show that R_1^j is an operator of Hilbert-Schmidt class for j large. For then, by the minimax principle for the eigenvalues of a compact positive self-adjoint operator, the n-th eigenvalue (with repetitions for multiplicity) of $R^*R = R_1^* \cdot S^* \cdot S \cdot R_1$ is less than $\| S \|^2$ times the n-th eigenvalue in decreasing order of R_1^2. Since R_1^j is of Hilbert-Schmidt type, $\mathrm{Tr}(R_1^{2j}) < \infty$, where $\mathrm{Tr}(T)$ is the trace of the compact positive operator T. It follows that $\mathrm{Tr}((R^*R)^j) < \infty$. By a theorem of Ky Fan [12], it follows that $\mathrm{Tr}((R^*)^j R^j) \leq \mathrm{Tr}((R^*R)^j) < \infty$. Thus $(R^*)^j$ and hence also its adjoint R^j are operators of Hilbert-Schmidt type.

Let B be an open disk in E^n containing the closure of G_0 in its interior. If $H_m(G_0)$ and $H_m(B)$ are the spaces of functions on G_0 and B respectively satisfying the m-th order null Dirichlet conditions in the variational sense, we may describe these spaces as the closures of $C_c^\infty(G_0)$ and $C_c^\infty(B)$ in the norm $\| f \|_m{}^2 = \sum_{|\beta| \leq m} (D^\beta f, D^\beta f)$ associated with the inner product $[f,g]_m = \sum_{|\beta| \leq m} (D^\beta f, D^\beta g)$. In particular, $H_m(G_0)$ may be taken as a closed subspace of $H_m(B)$. If we define the Dirichlet form associated with $(L_s + (-1^m kI)$ as $d(f,g) = \int_{G_0} \{(-1)^m L_s f + kf\}\bar{g}\,dx$, it follows by integration by parts and the

Schwarz inequality that for a suitable positive constant c_0, $d(f,f) \geqq c_0 \| f \|_m{}^2$. Let R_2 be the inverse of the Friedrichs extension of the differential operator $\sum_{|\beta| \leqq m} (-1)^{|\beta|} D^\beta (D^\beta u)$. R_1 and R_2 are characterized, respectively, by the equations:

$$d(R_1 f, \phi) = (-1)^m (f, \phi), \ \phi \text{ in } H_m(G_0)\,;\ R_1 f \in H_m(G_0)\,;$$

$$[R_2 f, \phi]_m = (f, \phi), \ \phi \in H_m(B)\,;\ R_2 f \in H_m(B).$$

It follows that for f in $H(G_0)$,

$$\begin{aligned}(-1)^m (R_1 f, f) &= d(R_1 f, R_1 f) = \sup\{ | d(R_1 f, \phi) |^2 \cdot d(\phi,\phi)^{-1} : \phi \in C_c{}^\infty (G_0)\} \\ &= \sup\{ | (f,\phi) |^2 \cdot d(\phi,\phi)^{-1} : \phi \in C_c{}^\infty (G_0)\} \\ &\leqq \sup\{ | (f,\phi) |^2 \cdot c_0^{-1} \| \phi \|_m{}^{-2} : \phi \in C_c{}^\infty (G_0)\} \\ &= c_0^{-1} \sup\{ | [R_2 f, \phi]_m |^2 \cdot \| \phi \|_m{}^{-2} : \phi \in C_c{}^\infty (G_0)\} \\ &\leqq c_0^{-1} [R_2 f, R_2 f]_m = c_0^{-1} (R_2 f, f).\end{aligned}$$

This last chain of inequalities yields the conclusion that in the Hilbert space $L^2(G_0)$, we have $0 \leqq (-1)^m R_1 \leqq c_0^{-1}(PR_2P)$. But by the remarks preceeding Theorem 1, for $2mj > n/2$, $(PR_2P)^j$ is an operator of Hilbert-Schmidt type. Hence so is $R_1{}^j$, and the lemma is proved.

Proof of Theorem 1 *continued.* To complete the proof, we must show that the eigenfunctions of L under null Dirichlet conditions of order m are dense in $C^\infty(G_0)$. It suffices to show, for any ψ in $C_c{}^\infty(G)$, a non-negative integer j_0 and a compact subset K of G_0, that ψ can be approximated by a linear combination of eigenfunctions of L in $C^{j_0}(K)$. Let j be an integer such that $2mj > n/2 + j_0$. It is a standard result of the theory of elliptic equations (see for example the writer's paper in the Annals of Mathematics Study, No. 33, Princeton, 1954) that R^j for such j is a bounded linear mapping of $L^2(G_0)$ into $C^{j_0}(K)$. Let $\phi = (L + (-1)^m kI)^j \psi$. Since ϕ lies in $L^2(G_0)$, there exists a finite family of eigenfunctions $\{u_r\}$ of the Dirichlet problem for L on G_0 such that $\| \phi - \sum_r u_r \|_{L^2(G_0)} < \epsilon$. For each eigenvalue ζ of L, $\zeta \neq (-1)^{m+1} k$. If u is an eigenfunction of order $\leqq s$ with eigenvalue ζ, then $u = (L + (-1)^m kI)^j v$, where v is a finite sum of eigenfunctions with eigenvalue ζ of order $\leqq s$. Indeed let V_s be the finite subspace of $L^2(G_0)$ spanned by the eigenfunctions of L with eigenvalue ζ of order $\leqq s$. Then L maps V_s into itself, and $(L - \zeta I)^s(V_s) = \{0\}$. Thus ζ is the only point in the spectrum of L on V_s, and $(L + (-1)^m kI)^{-1}$ is well-defined and maps V_s onto itself. Iterating j times, we obtain our previous observation. It follows

that for each u_r, there exists a finite sum v_r of eigenfunctions of L with the same eigenvalue such that $(L+(-1)^m kI)v_r = u_r$. But then

$$\psi - \sum_r v_r = R^j(\phi - \sum_r u_r).$$

By our previous remark,

$$\sup_{x\in K} | D^\alpha(\psi - \sum_r v_r)(x) | \leqq M_{\alpha,K} \| \phi - \sum_r u_r \|_{L^2(G_0)} \leqq M_{\alpha,K}\epsilon.$$

If we now choose ϵ sufficiently small and a corersponding set of eigenfunctions $\{u_r\}$, we may make any finite number of the bounds $M_{\alpha,K}\epsilon$ arbitrarily small.

THEOREM 2. *Let L be an elliptic differential operator with infinitely differentiable coefficients in the interior of an open set G of E^n and satisfying the (U.C.P.S.) property above. Then the eigenfunctions of L on G are dense in $C^\infty(G)$. Dually, if w is a distribution with compact support in G such that $w(u) = 0$ for all eigenfunctions u of L on G, then $w = 0$.*

Proof of Theorem 2. Since $C_c^\infty(G)$ is dense in $C^\infty(G)$, it suffices to approximate ψ in $C_c^\infty(G)$, uniformly with all derivatives up to some given order on a compact set K. By Lemma 2, there exists a pre-compact open subset G_0 of G containing K and such that $G - G_0$ has no compact components. Since K is a compact subset of G_0, by Theorem 1 we can approximate ψ in $C_c^\infty(G_0)$ by a finite sum of eigenfunctions u_r of L on G_0. But by Lemma 1, each of these eigenfunctions can be approximated with arbitrary accuracy in $C^\infty(K)$ by an eigenfunction u_r' of L on G, since $G - G_0$ has no compact components. Combining these approximations, the theorem is proved.

2. The present section is concerned, as we have remarked in the Introduction, with the proof of an extension of Bochner's theorem to eigenfunction expanstions for a partial differential operator L, not necessarily elliptic, on an open subset G of E^n.

Let L be of order r $(r \geqq 1)$, $L = \sum_{|\alpha|\leqq r} a_\alpha(x) D^\alpha$, We shall assume once more that the coefficients of L are infinitely differentiable at each point of G. The adjoint operator L' is defined by $L'u = \sum_{|\alpha|\leqq r} (-1)^{|\alpha|} D^\alpha(\bar{a}_\alpha(x)u)$, and $\bar{L}$ is the operator obtained from L by taking the complex conjugates of the coefficients.

Let $K(x,y)$ be a continuous function on $G \times G$. The function K is said to be positive definite if for every finite set $\{x_1, \cdots, x_s\}$ of points of G and a corresponding set of complex numbers $\{\zeta_1, \cdots, \zeta_s\}$, we have

$$\sum_{j,k=1}^{s} K(x_j, x_k)\zeta_j\bar{\zeta}_k \geqq 0. \tag{3}$$

If K is positive definite, the inner product defined by

$$\langle f, g\rangle = \int_{G\times G} K(x,y) f(x)\bar{g}(y)\,dx\,dy \tag{4}$$

for f and g in $C_c^\infty(G_0)$, defines a semi-norm $\| f \|_K = \langle f, f\rangle^{\frac{1}{2}}$ on $C_c^\infty(G_0)$, since by (3), $\langle f, f\rangle \geqq 0$, and by standard arguments, $|\langle f, g\rangle| \leqq \| f \|_K \cdot \| g \|_K$ and $\| f + g \|_K \leqq \| f \|_K + \| g \|_K$.

Let N be the linear subset of $C_c^\infty(G)$ of those f for which $\| f \|_K = 0$. Since $\langle f, h\rangle = 0$ for f in N and h in $C_c^\infty(G)$, the inner product $\langle -, -\rangle$ is defined on the equivalence classes of $C_c^\infty(G)$ modulo N and yields a pre-Hilbert space structure on $C_c^\infty(G)/N$. Let the Hilbert space H be the completion of $C_c^\infty(G)/N$ with respect to $\| - \|_K$.

Suppose that we are given a linear endomorphism T_0 of $C_c^\infty(G)$ and another linear endomorphism $T_0^\#$ of $C_c^\infty(G)$ which is adjoint to T_0 with respect to the K-inner product, i. e.,

$$\langle T_0, f, g\rangle = \langle f, T_0^\# g\rangle \tag{5}$$

for all f and g in $C_c^\infty(G)$. Then for $f \in N$, (5) implies that $\langle T_0 f, g\rangle = 0$ for all g in $C_c^\infty(G)$, i. e., $T_0 f \in N$. Thus $T_0(N) \subset N$, $T_0^\#(N) \subset N$. As a result T_0 and $T_0^\#$ induce linear endomorphisms of $C_c^\infty(G)/N$. We denote these endomorphisms by T and $T^\#$ and consider them as linear transformations defined on the dense subset $C_c^\infty(G)/N$ of H and with range in H. If we denote the inner product in H by $\langle \cdot, \cdot\rangle$, then (5) implies that

$$\langle Tu, v\rangle = \langle u, T^\# v\rangle\,;\ u, v \in D(T) = D(T^\#). \tag{6}$$

Definition 1. T_0 is said to be symmetric with respect to K if we may choose $T_0^\# = T_0$.

In particular, the partial differential operator $\bar{L}'$ is symmetric with respect to K if and only if it satisfies the condition (2) given in the Introduction.

Definition 2. T_0 is said to be subnormal if there exists a Hilbert space H_1 containing H as a closed subspace and a normal operator T_1 in H_1 such that $T \subseteq T_1$.

Definition 3. If u is a locally integrable function on G, then u is said to be an eigenfunction of T_0', the dual of T_0, with eigenvalue ζ, a complex number, if

$$(7) \qquad \int_G u(x)(T_0 f)(x)\,dx = \zeta \int_G u(x) f(x)\,dx$$

for all f in $C_c^\infty(G)$.

Remark. In the present section, we consider only eigenfunctions of order one in the sense of section 1 of the present paper, or [8]. Further, while we allow eigenfunctions in the distribution sense, we restrict ourselves to locally integrable functions instead of allowing general distributions.

Definition 4. If $\psi(x,y,\lambda)$ is a function on $G \times G \times R^1$ integrable on compact subsets of $G \times G$ for each λ in R^1, then ψ is said to be an elementary kernel for T_0 on G if for each pair f and g in $C_c^\infty(G)$,

$$(8)_1 \qquad \int_{G\times G} \psi(x,y,\lambda)(T_0 f)(x)\bar{g}(y)\,dx\,dy = \int_{G\times G} \psi(x,y,\lambda) f(x)(\overline{T_0 g})(y)\,dx\,dy = \lambda \int_{G\times G} \psi(x,y,\lambda) f(x)\bar{g}(y)\,dx\,dy.$$

$$(8)_2 \qquad \int_{G\times G} \psi(x,y,\lambda) f(x)\bar{f}(y)\,dx\,dy \geqq 0,$$

for all λ in R^1.

(To obtain a corresponding definition for complex eigenvalues ζ, we replace equation $(8)_1$ by two equations,

$$(8)_3 \qquad \int_{G\times G} \psi(x,y,\zeta)(T_0 f)(x)\bar{g}(y)\,dx\,dy = \zeta \int_{G\times G} \psi(x,y,\zeta) f(x)\bar{g}(y)\,dx\,dy,$$

and

$$(8)_4 \qquad \int_{G\times G} \psi(x,y,\zeta) f(x)(\overline{T_0 g})\,dx\,dy = \bar{\zeta} \int_{G\times G} \psi(x,y,\zeta) f(x)\bar{g}(y)\,dx\,dy.)$$

THEOREM 3. *Let $K(x,y)$ be a continuous function on $G \times G$, T_0 a continuous linear endomorphism of $C_c^\infty(G)$. Then K is positive definite on G and T_0 is symmetric with respect to K if and only if there exist a positive finite Borel measure m on R^1, an elementary kernel $\psi(x,y,\lambda)$ for T_0 on G, and a (possibly infinite) sequence $\{\phi_j(x,\lambda)\}$ of eigenfunctions of the dual of T_0 on G with eigenvalue λ for each λ in R^1 such that:*

(a) *$\psi(x,y,\lambda)$ is measurable on $G_B \times G \times R^1$ with respect to the measure*

$(dx \cdot dy \cdot m(d\lambda))$. *Each* ϕ_j *is measurable on* $G \times R^1$ *with respect to* $dx \cdot m(d\lambda)$. *For each* j, $\int_{R^1} |\phi_j(x,\lambda)|^2 m(d\lambda)$ *is bounded a.e. on every compact subset* C *of* G, *and we have*

$$(9) \qquad \sum_j \text{ess. sup.}_{x \in C} \int_{R^1} |\phi_j(x,\lambda)|^2 m(d\lambda) < \infty.$$

In addition,

$$(10) \qquad \text{ess. sup.}_{x,y \in C} \int_{R^1} |\psi(x,y,\lambda)| m(d\lambda) < \infty.$$

(b) *There exists the representation*

$$\psi(x,y,\lambda) = \sum_j \phi_j(x,\lambda) \bar{\phi}_j(y,\lambda),$$

the sum being absolutely convergent outside a set of $dx \cdot dy \cdot m(d\lambda)$ *measure null on* $G \times G \times R^1$, *and convergent in* $L^1(m)$ *uniformly for* x *and* y *in any compact subset of* G.

(c) *For almost all* x *and* y *in* G,

$$K(x,y) = \int_{R^1} \psi(x,y,\lambda) m(d\lambda) = \sum_j \int_{R^1} \phi_j(x,\lambda) \bar{\phi}_j(y,\lambda) m(d\lambda),$$

each integral and the sum being uniformly absolutely convergent a.e. on every compact subset of $G \times G$.

(d) *If* C *is a compact subset of* G, d_0 *its distance from* $E^n - G$, h *an element of* E^n *with* $|h| < d_0$, *then*

$$\sum_j \text{ess. sup.}_{x \in C} \int_{R^1} |\phi_j(x+h) - \phi_j(x)|^2 m(d\lambda) = r_C(h) < \infty,$$

where $r_C(h) \to 0$ *as* $h \to 0$.

THEOREM 4. *Let* L *be a partial differential operator with infinitely differentiable coefficients in* G *and with the property that for each* λ *in* R^1, *every distribution solution of* $(L - \lambda I)\phi = 0$ *is an infinitely differentiable function. If* $T_0 = \bar{L}'$ *satisfies the conditions of Theorem* 1, *i.e., is symmetric with respect to a continuous positive definite function* K *on* $G \times G$, *then the elementary kernel* $\psi(x,y,\lambda)$ *may be chosen infinitely differentiable in* $G \times G$ *for each* λ, *each of the eigenfunctions* $\phi_j(x,\lambda)$ *may be chosen infinitely differentiable in* G *for each* λ *in* R^1, $L_x\psi = \bar{L}_y\psi = \lambda\psi$, $L\phi_j = \lambda\phi_j$ *for all* λ. *In this case,*

$$\psi(x,y,\lambda)=\sum_j \phi_j(x,\lambda)\bar{\phi}_j(y,\lambda), \tag{11}$$

the sum converging uniformly for x and y in any compact subset of G for each λ in R^1. For fixed λ in R^1 and y in G, the right-hand side of (11) *converges to ψ in $C^\infty(G)$ as a function of x in G. Similarly, for fixed λ in R^1 and x in G, the right-hand side of* (11) *converges to ψ in $C^\infty(G)$ as a function of y in G.*

THEOREM 5. *If K is a continuous positive definite function on G and T_0 is subnormal with respect to K, then one may obtain a representation of K by a positive measure m on C^1, a complex elementary kernel $\psi(x,y,\zeta)$ for T_0 on G, and a sequence of eigenfunctions $\{\phi_j(x,\zeta)\}$ of the dual of T_0 with complex eigenvalues, for which conclusions* (a)-(d) *of Theorem* 1 *are satisfied with all integrations in $m(d\zeta)$ being taken over the complex plane C^1.*

Proof of Theorem 3. The fact that conditions (a), (b), (c), and (d) taken together imply that K is continuous and positive definite and that T_0 is symmetric with respect to K, follows by an elementary computation. We shall, therefore, restrict ourselves to the proof that, if K is continuous in $G\times G$ and positive definite, and if T_0 is symmetric with respect to K, then conditions (a), (b), (c), and (d) must hold.

If T_0 is symmetric with respect to K, the corresponding operator T in the Hilbert space H, defined earlier in this section, is a densely defined symmetric operator in H. By a theorem of Neumark ([1]), there exists a Hilbert space H_1 containing H as a closed subspace and a self-adjoint operator T_1 in H_1 whose restriction to $D(T_1)\cap H$ contains the operator T. Let $\{E_\lambda\}$ be the spectral family of T_1 in H_1. If u is any element of H_1, the cyclic subspace generated by u with respect to $\{E_\lambda\}$ is defined as the subspace of H_1 spanned by the elements $E(S)u$, where S runs over the Borel subsets of R^1. It follows by a simple argument (see Lemma 3 of [7]) that it is possible to choose H_1 and T_1 such that H_1 is the direct sum of a countable family of orthogonal cyclic subspaces H_j corresponding to a sequence of elements $\{u_j\}$ of H_1. Let $m_j(S)=\langle E(S)u_j,u_j\rangle$, and set

$$m(S)=\sum_j 2^{-j}m_j(S) \tag{12}$$

for any Borel set S of R^1.

By a standard argument of the spectral theory of self-adjoint operators, there exists an unitary mapping U_j of H_j onto $L^2(m_j)$, where for a bounded function c on R^1, $U_j^{-1}(c)=\int_{R^1}c(\lambda)\,dE_\lambda u_j$. Further, if P_j is the orthogonal

projection of H_1 on its closed subspace H_j, $P_j(D(T_1)) = D(T_1) \cap H_j$. For u in $D(T_1)$, $P_jT_1u = T_1P_ju$, while $(U_jP_jT_1u)(\lambda) = \lambda(U_jP_ju)(\lambda)$ a.e. in m_j for each u in $D(T_1)$.

By the definition (12) of the measure m, m_j is absolutely continuous with respect to m. If h_j is the Radon-Nikodym derivative of m_j with respect to m, h_j is defined a.e. in m and $h_j \geqq 0$. For c in $L^2(m_j)$, put $S_jc = h_j^{\frac{1}{2}}c$. Then, S_j is an isometric mapping of $L^2(m_j)$ into $L^2(m)$, and $(S_jU_jP_jT_1u)(\lambda) = \lambda(S_jU_jP_ju)(\lambda)$ a.e. in m for each u in $D(T_1)$.

Let R be the mapping of $C_c^\infty(G)$ into H which sends a function f into its equivalence class in $C_c^\infty(G)/N$, where the latter is considered as a subset of H. If C is a fixed open subset precompact in G, then for $f \in C_c^\infty(C)$,

$$\| Rf \|_K{}^2 = \int_{G\times G} K(x,y)f(x)\bar{f}(y)\,dx\,dy \leqq a_C{}^2 \{\| f \|_{L^1(C)}\}^2,$$

where $a_C{}^2$ is the upper bound of $|K(x,y)|$ on $C \times C$.

We complete our notational definitions by setting

$$Q_jf = S_jU_jP_jRf, \qquad f \in C_c^\infty(G). \tag{13}$$

Q_j maps $C_c^\infty(G)$ into $L^2(m)$.

Since $H_1 = \sum_j \oplus H_j$, U_j is unitary, and S_j is isometric, we have

$$\sum_j \| Q_jf \|_{L^2(m)}{}^2 = \| Rf \|_K{}^2 \leqq a_C{}^2 \{\| f \|_{L^1(C)}\}^2, \qquad f \in C_c^\infty(C). \tag{14}$$

By continuity, Q_j may be extended from the dense subset $C_c^\infty(C)$ of $L^1(C)$ to a bounded linear transformation from $L^1(C)$ to $L^2(m)$ with the same bound. By a theorem of Dunford and Pettis [11], every bounded linear transformation on Q_j from $L^1(C)$ into $L^2(m)$ has an integral representation of the form

$$(Q_jf)(\lambda) = \int_G \phi_j(x,\lambda)f(x)\,dx, \qquad f \in L^1(C), \tag{15}$$

where $\phi_j(x,\lambda)$ is a measurable function on $C \times R^1$ with respect to the measure $dx \cdot m(d\lambda)$, and a.e. in G,

$$\int_{R^1} |\phi_j(x,\lambda)|^2\, m(d\lambda) \leqq b_{C,j}{}^2, \tag{16}$$

where $b_{C,j}$ is the norm of Q_j as a mapping from $L^1(C)$ into $L^2(m)$. By (14), $\sum_j b_{C,j}{}^2 \leqq a_C{}^2$, i.e.,

$$\sum_j \text{ess. sup.}_{x\in C} \int_{R^1} |\phi_j(x,\lambda)|^2\, m(d\lambda) \leqq a_C{}^2. \tag{17}$$

We now remark that if $C \subset C_1$, where C_1 is another precompact open subset of G, then the $\phi_j'(x,\lambda)$ defined for C_1 by the same procedure coincide on $C \times R^1$ with $\phi_j(x,\lambda)$ except on a set of $dx \cdot m(d\lambda)$ measure zero. Since G is the union of an increasing sequence of pre-compact subsets, we may define $\phi_j(x,\lambda)$ on $G \times R^1$ uniquely up to a set of $dx \cdot m(d\lambda)$ measure zero and satisfying (14) for every f in $C_c^\infty(G)$, and all the other conditions on every compact subset C of G.

If $f \in C_c^\infty(G)$,

$$(Q_jT_0f)(\lambda) = (S_jU_jP_jRT_0f)(\lambda) = (S_jU_jP_jTRf)(\lambda)$$
$$= (S_jU_jT_1P_jRf)(\lambda) = \lambda(S_jU_jP_jRf)(\lambda) = \lambda(Q_jf)(\lambda)$$

a.e. in m. Thus for each f in $C_c^\infty(G)$, there exists an m-null set $\pi(f)$ such that for $\lambda \in R^1 - \pi(f)$,

$$\int_G \phi_j(x,\lambda)(T_0f)(x)\,dx = \lambda \int_G \phi_j(x,\lambda)f(x)\,dx. \tag{18}$$

By an elementary proof given in [8], thre exists a dense denumerable set $\{f_k\}$ in $C_c^\infty(G)$. Let $\pi_k = \pi(f_k)$, $\pi = \bigcup_k \pi_k$. Then for $\lambda \in R^1 - \pi$, it follows from the continuity of T_0 as an endomorphism of $C_c^\infty(G)$, that (18) holds for all f in $C_c^\infty(G)$. If we set $\phi_j(x,\lambda) = 0$ for $\lambda \in \pi$ and all x in G, the change in ϕ_j affects its value only on an $(dx \cdot m(d\lambda))$-null set and leaves the measurability properties and the previously discussed properties of the ϕ_j unaltered. After the change, (18) holds for all f in $C_c^\infty(G)$ and all λ in R^1, i.e., $\phi_j(x,\lambda)$ is an eigenfunction of the dual of T_0 with eigenvalue λ in the sense of Definition 3 for every λ.

Let $q(x,\lambda) = \sum_j |\phi_j(x,\lambda)|^2$, $q_N(x,\lambda) = \sum_j |\phi_j(x,\lambda)|^2$. By (17)

$$\text{ess. sup.}_{x \in C} \int_{R^1} q_N(x,\lambda)\,m(d\lambda) \leqq a_C^2. \tag{19}$$

Since q_N is a monotone non-decreasing sequence of nonnegative functions converging everywhere to q as $N \to \infty$, it follows that q is a measurable function on $G \times R^1$ with respect to $dx \cdot m(d\lambda)$, finite a.e. with respect to that measure, for which

$$\text{ess. sup.}_{x \in C} \int_{R^1} q(x,\lambda)\,m(d\lambda) \leqq a_C^2 \tag{20}$$

for every precompact open subset C of G.

Let $\psi_N(x,y,\lambda) = \sum_{j \leqq N} \phi_j(x,\lambda)\bar{\phi}_j(y,\lambda)$. By the Schwarz inequality

$$|\psi_N(x,y,\lambda)-\psi_M(x,y,\lambda)| \leqq |q_N(x,\lambda)-q_M(x,\lambda)|^{\frac{1}{2}}\cdot|q_N(y,\lambda)-q_M(y,\lambda)|^{\frac{1}{2}}.$$

It follows that $\psi_N(x,y,\lambda)$ converges to a function $\psi(x,y,\lambda)$, measurable with respect to $dx\cdot dy\cdot m(d\lambda)$ on $G\times G\times R^1$ and satisfying the inequality.

$$(21) \qquad |\psi(x,y,\lambda)| \leqq [q(x,\lambda)]^{\frac{1}{2}}\cdot[q(y,\lambda)]^{\frac{1}{2}}.$$

If C is a precompact subset of G, let N_j be a null set in C such that for x in $C-N_j$,

$$\int_{R^1}|\phi_j(x,\lambda)|^2\, m(d\lambda) \leqq b_{C,j}^2.$$

On the complement of the null set $N=\bigcup_j N_j$, the series

$$\sum_j \int_{R^1}|\phi_j(x,\lambda)|^2\, m(d\lambda)$$

is convergent, and

$$\sum_{j=M}^{N}\sup{}_{x\in N}\int_{R^1}|\phi_j(x,\lambda)|^2\, m(d\lambda) \leqq \sum_{j=M}^{N} b_{C,j}^2,$$

with the terms on the right going to zero as M and $N\to\infty$. But,

$$\int_{R^1}|q_N(x,\lambda)-q_M(x,\lambda)|^2\, m(d\lambda) = \sum_{j=M}^{N}\int_{R^1}|\phi_j(x,\lambda)|^2\, m(d\lambda),$$

implies, then, that $q_N(x,\cdot)$ converges to a limit in $L^2(m)$ uniformly for x in N. This limit must obviously be $q(x,\cdot)$ since $q_N(x,\lambda)$ converges to $q(x,\lambda)$ for every x and λ. Turning to ψ_N, we see that

$$\int_{R^1}|\psi_N(x,y,\lambda)-\psi_M(x,y,\lambda)|\, m(d\lambda) \leqq \Big[\int_{R^1}|q_N(x,\lambda)-q_M(x,\lambda)|^2\, m(d\lambda)\Big] \cdot\Big[\int_{R^1}|q_N(y,\lambda)-q_M(y,\lambda)|^2\, m(d\lambda)\Big],$$

showing that $\psi_N(x,y,\cdot)$ converges to a limit in $L^1(m)$ uniformly for x and y in N. This limit must be $\psi(x,y,\cdot)$ a. e. on $G\times G$, since $\psi_N(x,y,\lambda)$ converges to $\psi(x,y,\lambda)$ on $G\times G\times R^1$. We have, in addition,

$$(22) \qquad \text{ess. sup.}_{x,y\in C}\int_{R^1}|\psi(x,y,\lambda)|\, m(d\lambda) < \infty.$$

Let f and g be arbitrary elements of $C_c^\infty(G)$. It follows from the above inequalities that

$$\int_{G\times G\times R^1}|\psi_N(x,y,\lambda)-\psi(x,y,\lambda)|\cdot|T_0 f(x)|\cdot|g(y)|\, dx\, dy\, m(d\lambda)$$

goes to zero as $N \to \infty$. It follows that there exists a null set $\pi_{f,g}$ with respect to m on R^1 and a subsequence $\{N_k\}$ such that

$$\int_{G\times G} |\psi(x,y,\lambda) - \psi_{N_k}(x,y,\lambda)| \cdot |T_0 f(x)| \cdot |g(y)|\, dx\, dy \to 0$$

as $k \to \infty$ for $\lambda \in R^1 - \pi_{f,g}$. Similarly (possibly choosing a subsequence),

$$\int_{G\times G} |\psi(x,y,\lambda) - \psi_{N_k}(x,y,\lambda)| \cdot |f(x)| \cdot |T_0 g(y)|\, dx\, dy \to 0$$

for λ in the complement of another m-null set $\pi'_{f,g}$, which we may assume the same as the first. Finally, we may assume (again possibly enlarging the m-null set $\pi_{f,g}$) that for the subsequence N_k,

$$\int_{G\times G} |\psi(x,y,\lambda) - \psi_{N_k}(x,y,\lambda)| \cdot |f(x)| \cdot |g(y)|\, dx\, dy \to 0 \text{ as } k \to \infty.$$

Thus we have

$$\int_{G\times G} \psi(x,y,\lambda) T_0 f(x) \bar{g}(y)\, dx\, dy = \lim_k \int_{G\times G} \psi_{N_k}(x,y,\lambda) T_0 f(x) \bar{g}(y)\, dx\, dy$$
$$= \lambda \lim_k \int_{G\times G} \psi_{N_k}(x,y,\lambda) f(x) \bar{g}(y)\, dx\, dy = \lambda \int_{G\times G} \psi(x,y,\lambda) f(x) \bar{g}(y)\, dx\, dy,$$

for λ outside $\pi_{f,g}$. By a similar argument,

$$\int_{G\times G} \psi(x,y,\lambda) f(x) (\overline{T_0 g})(y)\, dx\, dy = \lambda \int_{G\times G} \psi(x,y,\lambda) f(x) \bar{g}(y)\, dx\, dy,$$

for λ in the complement of $\pi_{f,g}$. Let f and g run independently through a dense denumerable set $\{f_k\}$ in $C_c^\infty(G)$, and let π be the union of a corresponding sequence of m-null sets $\pi_{f,g}$. In the complement of π, we have by a simple continuity argument,

$$\begin{aligned} (23) \qquad & \int_{G\times G} \psi(x,y,\lambda) (T_0 f)(x) \bar{g}(y)\, dx\, dy \\ &= \int_{G\times G} \psi(x,y,\lambda) f(x) (\overline{T_0 g})(y)\, dx\, dy \\ &= \lambda \int_{G\times G} \psi(x,y,\lambda) f(x) \bar{g}(y)\, dx\, dy, \end{aligned}$$

for all f and g in $C_c^\infty(G)$. If we set $\psi(x,y,\lambda) = 0$ on $G \times G \times \pi$, which is a null set with respect to $dx \cdot dy \cdot m(d\lambda)$, none of our previous conclusions are disturbed, and the equality (23) will hold after the change for all λ in R^1.

It then follows that $\psi(x,y,\lambda)$ is an elementary kernel for T_0 in the sense of Definition 4.

If we set $S(x,y)=\int_{R^1}\psi(x,y,\lambda)m(d\lambda)$, the inequality (22) implies that $S(x,y)$ is essentially bounded on every compact subset of $G\times G$. By an elementary analytical argument,

$$S(x,y)=\sum_j\int_{R^1}\phi_j(x,\lambda)\,\bar{\phi}_j(y,\lambda)m(d\lambda),$$

with each integral, as well as the sum, being uniformly absolutely convergent a. e. on each compact subset of $G\times G$. To complete the verification of condition (a) of Theorem 1, we must show that $S(x,y)=K(x,y)$ a. e. on $G\times G$. Let f and g be two elements of $C_c^\infty(G)$. By the Fubini theorem,

$$\int_{G\times G}S(x,y)f(x)\bar{g}(y)\,dx\,dy$$

$$=\lim_N\sum_{j\leqq N}\int_{R^1}\Big(\int_G\phi_j(x,\lambda)f(x)\,dx\Big)\cdot\Big(\int_G\bar{\phi}_j(y,\lambda)\bar{g}(y)\,dy\Big)$$

$$=\sum_j\int_{R^1}Q_j(f)(\lambda)Q_j(g)(\lambda)m(d\lambda)=\langle Rf,Rg\rangle.$$

But by the definition of the K-inner product,

$$\langle Rf,Rg\rangle=\int_{G\times G}K(x,y)f(x)\bar{g}(y)\,dx\,dy.$$

Since the finite linear combinations of products $f(x)\bar{g}(y)$ with f and g in $C_c^\infty(G)$ are dense in $L^2(C\times C)$ for combat subsets C of G, and since both $K(x,y)$ and $S(x,y)$ are essentially uniformly bounded on any compact subset of $G\times G$, the equality,

$$\int_{G\times G}[K(x,y)-S(x,y)]f(x)\bar{g}(y)\,dx\,dy=0$$

for all f and g in $C_c^\infty(G)$, implies that $K(x,y)=S(x,y)$ a. e. in $G\times G$.

To complete the proof of Theorem 3, we must establish (d). Let C be a compact subset of G, d_0 its distance from E^n-G, h in E^n with $|h|=d<d_0$. The translation mapping $T_hf(x)=f(x-h)$ is a continuous linear mapping of $C_c^\infty(C)$ into $C_c^\infty(G)$. For f in $C_c^\infty(C)$, we have

$$\begin{aligned}\| RT_hf - Rf \|_K{}^2 &= \int_{G\times G} K(x,y)[f(x-h)-f(x)][\bar{f}(y-h)-\bar{f}(y)]\,dx\,dy\\ &= \int_{G\times G}[K(x+h,y+h)+K(x,y)-K(x+h,y)\\ &\qquad\qquad -K(x,y+b)]f(x)\bar{f}(y)\,dx\,dy\\ &\leqq \sup_{x,y\in N_d(C)} |K(x+h,y+h)+K(x,y)\\ &\qquad\qquad -K(x+h,y)-K(x,y+h)|\cdot \| f\|_{L^1(C)}{}^2,\end{aligned}$$

where $N_d(C)$ is the set of points at distance at most d from C.

If we set $r_C(h)$ equal to the supremum term in the last inequality, we have

$$\| Q_jT_hf - Q_jf\|_{L^2(m)}{}^2 \leqq r_C(h)\| f\|_{L^1(C)}{}^2.$$

By our previous remarks, however,

$$\begin{aligned}(Q_jT_hf - Q_jf)(\lambda) &= \int_G \phi_j(x,\lambda)\cdot[f(x-h)-f(x)]\,dx\\ &= \int_G [q(x+h,\lambda)-q(x,\lambda)]f(x)\,dx.\end{aligned}$$

It follows from the Dunford-Pettis theorem that

$$\sum_j \text{ess. sup.}_{x\in C} \int_{R^1} |\phi_j(x+h)-\phi_j(x)|^2\, m(d\lambda) \leqq r_C(h),$$

while the fact that $r_C(h)\to 0$ follows from the continuity of K and the precompactness of $N_d(C)$.

Thus the proof of Theorem 3 is complete. Note that if $T_0 = \bar{L}'$, where L is a partial differential operator on G, then the eigenfunctions of the dual of T_0 are precisely the eigenfunctions of L, locally integrable solutions of $(L-\lambda I)u = 0$ with differentiation taken in the distribution sense.

Proof of Theorem 4. If every locally integrable solution of $(L-\lambda I)u = 0$, for a fixed λ, lies in $C^\infty(G)$, then the identity mapping J of the space of such solutions, with the inductive limit topology induced by the $L^1(C)$-norm for compact subsets C of G, into $C^\infty(G)$, is a closed linear mapping from an LF-space into an F-space. Applying the closed graph theorem, which is an easy consequence of the closed graph theorem for mappings of F-spaces, J is continuous. Thus, given a compact subset C of G and an integer $j \geqq 0$, there is a compact subset C_1 of G and a constant $k_{C,j}$ such that

$$|D^\alpha u(x)| \leqq \int_{C^1} |u(x)|\,dx, \qquad x\in C, \tag{24}$$

for every locally integrable weak solution u of $(L-\lambda I)u = 0$.

Consider the N-th partial sum $\psi_N(x,y,\lambda)$ of (11). Since by the hypothesis of the present theorem, $\phi_j(\cdot,\lambda)$ for each fixed λ is essentially in $C^\infty(G)$, we may assume that each $\phi_j(\cdot,\lambda)$ is actually in $C^\infty(G)$ by replacing its value at each point x of G by the limit of its average on a family of spheres shrinking down to the point. The resulting function differs from the original ϕ_j only on a null-set in $G\times R^1$. In particular, each ψ_N is infinitely differentiable on $G\times G$ for each fixed λ in R^1. By (24) and the finiteness a.e. of $q(x,\lambda)$, using the argument of the proof of Theorem 3, it follows that except on a m-null set π in R^1,

$$\sum_{j\leqq N} |D^\alpha\phi_j(x,\lambda)|^2 < \infty \tag{25}$$

uniformly, for each fixed λ in $R^1-\pi$, for x in any compact subset C of G.

We may replace $\phi_j(x,\lambda)$ by zero on $G\times\pi$ without affecting any of its essential properties and assume that (25) holds for all λ. It follows by an elementary estimation that $D_x{}^\alpha D_x{}^\beta\psi_N(x,y,\lambda)$ converges for each fixed λ in R^1 and every α and β, uniformly on compact subsets of $G\times G$. Consequently, $\psi(x,y,\lambda)$, for fixed λ in R^1, lies in $C^\infty(G\times G)$, and the other conclusions of Theorem 4 follow.

The proof of Theorem 5 is essentially identical with that of Theorem 3, except that at the very beginning, the extension T_1 of T to the larger Hilbert space H_1 is normal, rather than self-adjoint. The only change that this necessitates is that all integrations in the spectral parameter must be taken over the complex plane instead of the real line R^1.

YALE UNIVERSITY.

REFERENCES.

[1] N. I. Achieser and I. M. Glasman, *Theorie der linearen Operatoren in Hilbert-Raum*, Berlin, 1954, Anhang I.

[2] Yu. M. Berezanski, "A generalization of Bochner's theorem to expansions in eigenfunctions of partial differential operators," *Dokladi Akademi Nauk*, vol. 110 (1956), pp. 893-896 (Russian).

[3] ———, "Eigenfunction expansions for self-adjoint operators," *Matematcheski Sbornik*, vol. 43 (1957), pp. 75-125 (Russian).

[4] F. E. Browder, "On the eigenfunctions and eigenvalues of the general linear elliptic differential operator," *Proceedings of the National Academy of Sciences*, vol. 39 (1953), pp. 433-439.

[5] ———, "La théorie spectrale des opérateurs aux derivées partielles du type elliptique," *Comptes Rendus*, vol. 246 (1958), pp. 526-528.

[6] ———, "Les opérateurs elliptiques et les problèmes mixtes," *ibid.*, vol. 246 (1958), pp. 365-381.

[7] ———, "Eigenfunction expansions for non-symmetric partial differential operators, I," *American Journal of Mathematics*, vol. 80 (1958), pp. 365-381.

[8] ———, "Eigenfunction expansions for non-symmetric partial differential operators, II," *ibid.*, vol. 81 (1959), pp. 1-22.

[9] ———, "On the spectral theory of elliptic differential operators, II," to appear.

[10] A. P. Calderon, "Uniqueness in the Cauchy problem for partial differential equations," *American Journal of Mathematics*, vol. 80 (1958), pp. 16-36.

[11] N. Dunford and B. J. Pettis, "Linear operations on summable functions," *Transactions of the American Mathematical Society*, vol. 47 (1940), pp. 323-392.

[12] K. Fan, "On a theorem of Weyl concerning eigenvalues of linear transformations," *Proceedings of the National Academy of Sciences*, vol. 35 (1949), pp. 652-655.

[13] M. Krein, "On a general method of decomposing positive definite Hermitian nuclei into elementary parts," *Dokladi Akademi Nauk*, vol. 52 (1946), pp. 3-6.

[14] P. D. Lax, "A stability theorem for solutions of abstract differential equations and its applications to the study of the local behaviour of solutions of elliptic equations," *Communications on Pure and Applied Mathematics*, vol. 8 (1956), pp. 747-766.

[15] B. Malgrange, "Existence et approximations des équations aux derivées partielles et des équations de convolution," *Annales de l'Institut Fourier de Grenoble*, vol. 6 (1956), pp. 271-355.

[16] L. Loomis, *An Introduction to Abstract Harmonic Analysis*, New York, 1953.

[17] D. V. Widder, *The Laplace Transform*, Princeton, 1941.

NUMERICAL EQUIVALENCE AND THE ZETA-FUNCTION OF A VARIETY.*

By J. H. SAMPSON and G. WASHNITZER.†

To Professor Zariski on his sixtieth birthday.

Introduction. One of the important problems of abstract algebraic geometry is to prove that there is a finite base for the group $\mathfrak{N}(V)$ of numerical equivalence classes of cycles on a variety V. It is known that the subgroup of $\mathfrak{N}(V)$ consisting of classes of divisors on V is finitely generated. That follows from the theorem of Néron-Severi [5], which shows that the group of algebraic equivalence classes of divisors on V is finitely generated. In characteristic zero it is a consequence of topological considerations that $\mathfrak{N}(V)$ is finitely generated; but in characteristic $p \neq 0$ very little is known in general about that group.

Given a non-singular projective variety V defined over a finite field with q elements, we establish here a connection between the theory of the base of $\mathfrak{N}(V \times V)$ and the Weil zeta-function $Z(u)$ of V: The assumption that $\mathfrak{N}(V \times V)$ (or a suitable part of it) is finitely generated permits us to deduce that $d \log Z(u)/du$ is a rational function of u. The proof is contained in §§1-5. It is closely bound up with the graphs in $V \times V$ of the q^{ν}-th power mappings of V onto itself.

Assuming that $d \log Z(u)/du$ is rational, but without any reference to the theory of the base, we show in § 6 that this function has only simple poles. (To establish the rationality of $Z(u)$ one would have to show that the residues at those poles are rational integers.) The argument of § 6 is based on properties of power series with integral coefficients. It is possible to reach the same conclusion (in a more conceptual way) by an analysis of the algebraic structure of the ring of correspondences of V, again invoking the theory of the base. That argument will be presented at a later time.

In § 7 we verify Weil's conjectured functional equation for $Z(u)$. It is a straightforward consequence of the canonical involution of $V \times V$. Finally,

---

* Received January 30, 1959.

† The authors were supported in part by a grant from the National Science Foundation.

in § 8 we sketch a sheaf-theoretic formulation of the argument of §§ 2-5. That formulation immediately sugegsts a number of generalizations, of which only bare mention is made here.

1. The zeta-function of a variety. Let V^r be a non-singular projective variety defined over a finite field K_1 containing q elements. For $\nu = 1, 2, 3$, etc. let K_ν denote the unique extension of K_1 in the universal domain containing q^ν elements. Let N_ν denote the number of points on V which are rational over K_ν, and let D_ν denote the number of positive zero-cycles of degree ν on V which are rational over K_1. We shall be concerned with the functions [1]

$$\Phi(u) = \sum_{\nu=1}^{\infty} N_\nu u^{\nu-1}, \qquad Z(u) = \sum_{\nu=0}^{\infty} D_\nu u^\nu \qquad (D_0 = 1). \tag{1}$$

They are related by the equation [2]

$$d \log Z(u)/du = \Phi(u). \tag{2}$$

2. Some preliminaries.

PROPOSITION 1. *Let U, W be non-singular projective varieties (complete), and let f be a regular rational transformation of U into W, with graph F in $U \times W$. Let X be a U-cycle and Y a W-cycle such that $X \times W, F, U \times Y$ intersect properly and such that $(X \times W) \cdot F$ and $F \cdot (U \times Y)$ are defined. Then* [3]

$$f(X \cdot f^{-1}(Y)) = f(X) \cdot Y. \tag{3}$$

Proof. Suppose first $\dim X \leqq \dim W$. The cycle $Q = (X \times W) \cdot F \cdot (U \times Y)$ is defined, and therefore $Z = X \cdot \mathrm{pr}_U[F \cdot (U \times Y)]$ is defined and equal to $\mathrm{pr}_U(Q)$ [F-VII, Th. 10, 16]. By definition, $Z = X \cdot f^{-1}(Y)$. Further, $(Z \times W) \cdot F$ is defined and equal to Q [F-VII, Th. 17, Cor. 3]. Then $f(X \cdot f^{-1}(Y)) = f(Z) = \mathrm{pr}_W(Q) = \mathrm{pr}_W\{[F \cdot (X \times W)] \cdot (U \times Y)\}$, which in turn is $\mathrm{pr}_W[F \cdot (X \times W)] \cdot Y = f(X) \cdot Y$ [F-VII, Th. 16]. If $\dim X > \dim W$, then both sides of (3) must be zero, from dimensional considerations.

Remark. In calculations with rational, algebraic or numerical equivalence

---

[1] $\Phi(u)$ and $Z(u)$ were introduced by Weil in C. A., II^e partie, §§ IV-V, for curves, and in [11] for arbitrary dimension r. See also V. A., § IX, No. 69 and [12].

[2] Proved for curves in C. A., II^e partie, Nos. 18, 19, 20. That demonstration holds *mutatis mutandis* for any dimension r.

[3] Notation essentially as in V. A., § 1, No. 3: $f(X) = \mathrm{pr}_W[F \cdot (X \times W)]$ and $f^{-1}(Y) = \mathrm{pr}_U[F \cdot (U \times Y)]$, etc.

classes of cycles it is always possible to find representative cycles for which the conditions of Proposition 1 are fulfilled, in virtue of results of W.-L. Chow [2, Lemma 2, Corollary 4, § 4 and Lemma 4, § 6]. Hence formula (3) is of unrestricted validity when applied to such equivalence classes.

PROPOSITION 2. *Let U, W, f be as in Proposition 1, with f now assumed purely inseparable and one-to-one. Let Y be a subvariety of W. Then the cycle $f^{-1}(Y)$ is always defined. K being a field of definition for f and Y, let y be a generic point of Y over K, and let y' be the unique point of U such that $f(y')=y$. If K is perfect, then y' has a locus Y' over K, and $f^{-1}(Y)=nY'$, where $n=(\deg f)/[K(y'):K(y)]$.*

Proof. F being the graph of f, one easily sees that every point of $F\cap(U\times Y)$ must be a specialization of (y',y) over K. Hence the first point. Since $f(y')=y$, we have $K(y',y)=K(y')$, which, by assumption, is a purely inseparable extension of $K(y)$. Consequently the ideal determined by y' over the algebraic closure of K has a basis with coefficients in a purely inseparable extension of K. If K is perfect, then $K(y')$ must be a regular extension. Thus (y',y) has a locus over K, which must be precisely $F\cap(U\times Y)$; and y' has a locus over K which is simply the projection of $F\cap(U\times Y)$ on U. Therefore $f^{-1}(Y)=\mathrm{pr}_U[F\cdot(U\times Y)]=nY'$, where n is the intersection multiplicity of F, $U\times Y$.

To calculate n, let Z be any subvariety of U. Then the cycle $f(Z)=\mathrm{pr}_W[F\cdot(Z\times W)]$ is always defined, clearly. The cycle $Z'=F\cdot(Z\times W)$ is a variety [F-VII, Th. 17]. Denote its projection on W by Z''. Then by definition $f(Z)=[Z':Z'']Z''$. Taking $Z=Y'$ we see that Z' is the locus of (y',y) over K. Consequently $f(Y')=[K(y'):K(y)]\cdot Y$. But from formula (3), with $X=U$, we have $f(f^{-1}(Y))=f(U)\cdot Y=(\deg f)\cdot Y$, whence $n\cdot f(Y')=(\deg f)\cdot Y$, or finally $n\cdot[K(y'):K(y)]=\deg f$.

3. The transformation φ. Returning now to the variety of § 1, we introduce the mapping ϕ of $V\times V$ onto itself defined for any point (u,v) of $V\times V$ by $\phi(u,v)=(u^q,v)$, where $u\to u^q$ is the q-th power mapping of V onto itself.[4] I. e., ϕ is the product of the q-th power mapping of V on the first factor of $V\times V$ and of the identity mapping on the second factor. ϕ is a regular rational one-to-one mapping of $V\times V$ onto itself, defined over K_1; it has degree q^r. Denoting the ν-th iterate of ϕ by ϕ^ν, we have $\phi^\nu(u,v)=(u^{q^\nu},v)$.

[4] If V is a subvariety of a projective space P^m, with a specified system of homogeneous coordinates in P^m, and if the point u has coordinates $u_0,\cdots,u_m$, then u^q denotes the point with coordinates $u_0{}^q,\cdots,u_m{}^q$. Similarly, u^{q^ν} has coordinates $u_0{}^{q^\nu},\cdots,u_m{}^{q^\nu}$ ($\nu=1,2,3$, etc.). Cf. F-VII, § 2.

In addition to ϕ we shall require the mapping σ of $V \times V$ defined by $\sigma(u,v) = (v,u)$ and also the q-th power mapping of $V \times V$ onto itself, denoted by τ: $\tau(u,v) = (u^q, v^q)$. Both σ and τ are purely inseparable regular rational transformations defined over K_1, and of course σ is biregular. ϕ, σ and τ are related by the identities

$$\sigma\sigma = 1, \qquad \sigma\phi\sigma\phi = \tau, \tag{4}$$

and more generally

$$\sigma\phi^\nu\sigma\phi^\nu = \tau^\nu, \tag{4'}$$

where 1 is the identity mapping of $V \times V$ and where ϕ^ν, τ^ν are the ν-fold iterates of ϕ, τ.

4. The diagonal cycle. Now let Δ_0 denote the diagonal in $V \times V$. From Proposition 2 it follows at once that the cycle[5] $\Delta_\nu = \phi^{-\nu}(\Delta_0)$ is defined and is a subvariety of $V \times V$ having K_1 as a field of definition ($\nu = 1, 2, 3$, etc.). It is moreover a non-singular subvariety of $V \times V$, as follows from the Jacobian criterion. The intersection set $\Delta_\nu \cap \Delta_0$ ($\nu > 0$) consists precisely of the points of Δ_0 which are rational over K_ν. The number of those points is therefore N_ν (cf. § 1 above). It is quickly seen that Δ_ν and Δ_0 are transversal at each point of intersection ($\nu > 0$). Therefore

$$N_\nu = \deg(\Delta_\nu \cdot \Delta_0) \qquad (\nu = 1, 2, 3, \cdots). \tag{5}$$

Now let $\mathfrak{N}(V \times V)$ denote the group of numerical equivalence classes of cycles on $V \times V$ (cf. Weil, F-IX, § 7); $\mathfrak{N}^r(V \times V)$ will stand for the subgroup consisting of classes of dimension r. Let $\mathfrak{d}_\nu$ denote the numerical equivalence class of the cycle Δ_ν ($\nu = 0, 1, 2, \cdots$). The $\mathfrak{d}_\nu$ are of course elements of $\mathfrak{N}^r(V \times V)$. Indicating the canonical scalar product in $\mathfrak{N}^r(V \times V)$ by the symbol $\langle \mathfrak{x}, \mathfrak{y} \rangle$, we have from (5)

$$N_\nu = \langle \mathfrak{d}_\nu, \mathfrak{d}_0 \rangle \qquad (\nu = 1, 2, 3, \cdots). \tag{6}$$

Each of the mappings ϕ^ν, σ, τ^ν induces an endomorphism of $\mathfrak{N}(V \times V)$ which preserves codimension. Those endomorphisms will be called $\phi^{\nu *}$, σ^*, $\tau^{\nu *}$ respectively. To describe them unambiguously, consider the mapping ϕ: Let $\mathfrak{x}$ be any numerical equivalence class, X a representative cycle. Then $\phi^{-1}(X)$ is defined, by Proposition 2, and by definition $\phi^*(\mathfrak{x})$ denotes its numerical equivalence class. Analogous definitions for $\phi^{\nu *}$, σ^*, $\tau^{\nu *}$. (In this

[5] $\phi^{-\nu}(\Delta_0)$ naturally stands for $(\phi^\nu)^{-1}(\Delta_0)$. We mention that, for the immediate purpose, we could equally well use the direct image cycle $\phi^\nu(\Delta_0)$. From § 2 above one easily verifies that $\phi^{-\nu}(\Delta_0) = \sigma(\phi^\nu(\Delta_0))$.

connection see Chow [2], § 6, especially Theorem 4.) It is clear from the definitions that

(7) $$\mathfrak{d}_\nu = \phi^{\nu *}(\mathfrak{d}_0)$$

and

(8) $$\phi^{\nu *} = (\phi^*)^\nu \qquad (\nu\text{-fold iterate of } \phi^*).$$

Hence

(9) $$N_\nu = \langle \phi^{\nu *}(\mathfrak{d}_0), \mathfrak{d}_0 \rangle = \langle (\phi^*)^\nu(\mathfrak{d}_0), \mathfrak{d}_0 \rangle.$$

Remark. In the expressions above it will be convenient to allow ν to take on the value zero. By ϕ^{0*} or $(\phi^*)^0$ we understand the identity endomorphism of $\mathfrak{N}(V \times V)$. The number N_0 defined by (6) or (9) for $\nu = 0$ is the self-intersection number of the diagonal Δ_0, hence the Euler-Poincaré characteristic of V. We shall also denote it by $\chi(V)$.

5. The rationality of $\Phi(u)$. As explained in the Introduction, our results concerning the zeta-function of V are based on a certain assumption concerning the group $\mathfrak{N}(V \times V)$. We now introduce that assumption explicitly. Write $\mathfrak{d}'_\nu = \sigma^*(\mathfrak{d}_\nu)$ $(\nu = 1, 2, \cdots)$, where, as above, σ^* is the involution of $\mathfrak{N}(V \times V)$ induced by the mapping σ. Of course $\mathfrak{d}'_0 = \mathfrak{d}_0$. Let G denote the subgroup of $\mathfrak{N}^r(V \times V)$ generated by the classes [6] $\mathfrak{d}_\nu$ and $\mathfrak{d}'_\nu$ $(\nu = 0, 1, 2, \cdots)$.

HYPOTHESIS. *It will henceforth be supposed that the group G is finitely generated.*[7]

Consider now the mapping τ^μ, which has degree $q^{2r\mu}$. Applying Proposition 2 we find at once that $\tau^{-\mu}(\Delta_\nu) = q^{r\mu}\Delta_\nu$. Similarly, writing $\Delta'_\nu = \sigma^{-1}(\Delta_\nu)$ (so that Δ'_ν is a representative cycle of $\mathfrak{d}'_\nu$), we have $\tau^{-\mu}(\Delta'_\nu) = q^{r\mu}\Delta'_\nu$. Therefore

(10) $$\tau^{\mu *} = (\tau^*)^\mu = q^{r\mu} \times \textit{identity in } G.$$

Again from Proposition 2 we obtain $\phi^{-1}(\Delta'_\nu) = q^r\Delta'_{\nu-1}$ $(\nu > 0)$; and of course $\phi^{-1}(\Delta_\nu) = \Delta_{\nu+1}$. Therefore ϕ^* maps G into itself. Since $\sigma^*\sigma^* = \text{identity}$, σ^* also maps G into itself. In what follows we shall be concerned solely with the action of ϕ^* and σ^* in G.

The group $\mathfrak{N}(V \times V)$ is free from torsion. Therefore, because of our hypothesis, G must be a free group, say of rank ρ. The endomorphism ϕ^*

---

[6] The classes $\mathfrak{d}'_\nu$ are included in G to ensure that σ^* maps G into itself. They will not play an essential rôle until No. 7 below.

[7] For $r = 1$ the finiteness is an immediate consequence of the Severi-Néron theory of the base (Néron [5], § 11, Theorem 2).

must consequently satisfy its characteristic equation. I. e., there exist rational integers $e_1, \cdots, e_\rho$ such that

$$(11) \qquad (\phi^*)^\nu + e_1(\phi^*)^{\nu-1} + \cdots + e_\rho(\phi^*)^{\nu-\rho} = 0 \text{ in } G$$

for every $\nu \geqq \rho$.[8] From (9) we obtain

$$(12) \qquad N_\nu + e_1 N_{\nu-1} + \cdots + e_\rho N_{\nu-\rho} = 0 \qquad (\nu \geqq \rho),$$

which is a linear difference equation for the numbers N_ν $(\nu \geqq 0)$. The rationality of the function $\Phi(u)$ defined by (1) is an immediate consequence of (12).

6. The functional form of $\Phi(u)$. We now show that the rationality of $\Phi(u)$ implies that it has simple poles. The argument of this section is based on certain properties of power series with integral coefficients; it is independent of the finiteness assumption made in § 5 above.

Let us temporarily write $\Phi_1(u)$ for $\Phi(u)$. If we now replace the ground field K_1 by one of the extensions K_h, then $\Phi_1(u)$ is replaced by the corresponding function (cf. § 1)

$$\Phi_h(u) = \sum_{\nu=1}^{\infty} N_{\nu h} u^{\nu-1} \qquad (h = 1, 2, 3, \cdots).$$

From (2) it follows that $\exp\{\int_0^u \Phi_h(u)\,du\}$ is a power series with *integral* coefficients, being the zeta-function of the variety V with reference to K_h. The hypotheses of the following theorem are therefore satisfied by $\Phi(u)$:

THEOREM 1. *Let $R(x) = \sum_{\nu=1}^{\infty} a_\nu x^{\nu-1}$ be a power series with integral coefficients which represents a rational function of x. For $h = 1, 2, 3$, etc. set $R_h(x) = \sum_{\nu=1}^{\infty} a_{\nu h} x^{\nu-1}$, and suppose that for each h the function $\exp\{\int_0^x R_h(x)\,dx\}$ has a representation as a power series in x with integral coefficients. Then $R(x)$ has a partial fraction decomposition of the form*

$$R(x) = \gamma_1/(1-\alpha_1 x) + \cdots + \gamma_s/(1-\alpha_s x),$$

where $\alpha_1, \cdots, \alpha_s$ and $\gamma_1, \cdots, \gamma_s$ are algebraic numbers. The α_i must in fact be algebraic integers.

Proof. First we recall that the rationality of $R(x) = R_1(x)$ implies that the coefficients a_ν satisfy a linear difference equation *for all large* ν.

---

[8] One could equally well use the minimal equation of ϕ^* in G.

I. e., there exists a relation of the form $c_0a_\nu + \cdots + c_\rho a_{\nu-\rho} = 0$ for all large ν, where $c_0, c_1, \cdots, c_\rho$ are fixed rational integers. (We assume that ρ has the minimum possible value.) If the c_j are relatively prime and $c_0 > 0$, then it is rather easily seen that $c_0 = 1$, since the a_ν are all integers. Hence, our relation has the form $a_\nu + c_1a_{\nu-1} + \cdots + c_\rho a_{\nu-\rho} = 0$. Let $\alpha_1, \cdots, \alpha_s$ be the distinct roots of the equation $\xi^\rho + c_1\xi^{\rho-1} + \cdots + c_\rho = 0$. The α_i are thus algebraic integers. Now by solving the difference equation above (for large ν), we can reconstruct the function $R(x)$, apart from a polynomial. It is readily seen that $R(x)$ must have a partial fraction decomposition of the form

$$R(x) = \sum \gamma_j/(1-\alpha_jx)^{m_j} + P(x), \tag{13}$$

where the α_j are as above (but possibly repeated for several exponents m_j), where the γ_j are algebraic numbers, and where $P(x)$ is a polynomial with integral coefficients.

Consider now the integral power series

$$\exp\{\int_0^x R(x)\,dx\} = \exp\{\sum_{\nu=1}^{\infty} (a_\nu/\nu)x^\nu\} = \prod_{\nu=1}^{\infty} \exp\{(a_\nu/\nu)x^\nu\}.$$

Let p be any prime. From the infinite product expansion it is easily seen that the coefficient of x^p in the power series expansion is $(a_1{}^p/p!) + (a_p/p) + Q$, where Q is a rational number whose denominator does not contain p. Then, since $p!Q$ is an integer, so is $(p-1)!Q$. Consequently, $a_1{}^p + (p-1)!\,a_p \equiv 0 \pmod p$, whence $a_1 \equiv a_p \pmod p$ (congruences of Wilson and Fermat). The same argument applied to $R_h(x)$ instead of $R_1(x)$ yields

$$a_h \equiv a_{hp} \pmod p \tag{14}$$

for all primes p and all $h = 1, 2, 3,$ etc.

We now compute the coefficients of x^{h-1} and x^{hp-1} from (13). For x^{h-1} we obtain

$$\sum \gamma_j\alpha_j{}^{h-1}m_j(m_j+1)\cdots(m_j+h-2)/(h-1)! + b_{h-1}, \tag{15}$$

where b_{h-1} is the coefficient of x^{h-1} in the polynomial $P(x)$. For all large p the coefficient of x^{hp-1} is

$$\sum \gamma_j\alpha_j{}^{hp-1}m_j(m_j+1)\cdots(m_j+hp-2)/(hp-1)!. \tag{16}$$

Now, for $h < p$, $(hp-1)!$ contains the factor p^{h-1} but not p^h. If $1 < m < p$, then the product $m(m+1)\cdots(m+hp-2)$ contains the factor p^h. Thus

$$m_j(m_j+1)\cdots(m_j+hp-2)/(hp-1)! \equiv 0 \pmod p \textit{ for } p \gg 0,\ m_j \neq 1. \tag{17}$$

Let E be the number field generated by the numbers α_i, γ_j. Let $\mathfrak{p}$ be a prime ideal in E of degree 1 with associated rational prime p, assumed large. By Fermat's theorem we have $\alpha_j^{hp} = (\alpha_j^h)^{N\mathfrak{p}} \equiv \alpha_j^h \pmod{\mathfrak{p}}$. Hence from (16), which is equal to a_{hp} for large p, we obtain

$$a_{hp} \equiv \sum_{(m_j=1)} \gamma_j \alpha_j^{h-1} \pmod{\mathfrak{p}}$$

for all primes $\mathfrak{p}$ of degree 1 with large $N\mathfrak{p} = p$ (the sum is to be extended over all terms for which $m_j = 1$). From this fact and from (14), (15) there follows

$$\sum_{(m_j>1)} \gamma_j \alpha_j^{h-1} m_j(m_j+1) \cdots (m_j+h-2)/(h-1)! + b_{h-1} \equiv 0 \pmod{\mathfrak{p}}, \tag{18}$$

the sum being over all terms for which $m_j > 1$. Since this congruence holds for infinitely many primes $\mathfrak{p}$,[9] we conclude that the left member of (18) is equal to zero for all h. But the left member of (18) is precisely the contribution to the coefficient a_h of x^{h-1} in $R(x)$ from the terms

$$\sum_{(m_j>1)} \gamma_j/(1-\alpha_j x)^{m_j} + P(x) \tag{19}$$

in the partial fraction decomposition (13). The contribution of (19) to $R(x)$ is therefore zero, which proves Theorem 1.

Solving (12) for the N_ν and applying Theorem 1, we find that $\Phi(u)$ must have the form

$$\Phi(u) = \beta_1\alpha_1/(1-\alpha_1 u) + \cdots + \beta_t\alpha_t/(1-\alpha_t u), \tag{20}$$

where now $\alpha_1, \cdots, \alpha_t$ are the *distinct* roots of the equation

$$x^\rho + e_1 x^{\rho-1} + \cdots + e_\rho = 0, \tag{21}$$

the e_j being as in (11) and (12). The β_j are algebraic numbers which must satisfy the relation

$$N_\nu = \sum_{j=1}^{t} \beta_j \alpha_j^\nu \tag{22}$$

for all $\nu = 0, 1, 2$, etc. We note in particular that

$$\chi(V) = N_0 = \beta_1 + \cdots + \beta_t. \tag{23}$$

The zeta-function itself must have the form

$$Z(u) = \prod_{j=1}^{t} (1-\alpha_j u)^{-\beta_j}, \tag{24}$$

---

[9] See e.g., Hecke [3], Satz. 126, p. 165.

suitable branches being chosen if the β_j are not rational integers. They presumably are. We note that

$$(25) \qquad N_\nu \equiv N_{\nu p} \pmod p$$

for $\nu = 1, 2, 3$, etc. and all rational primes p, as follows from (14).

7. The functional equation of $Z(u)$. We return now to the group G defined in § 5 and to the endomorphisms ϕ^* and σ^*. From (4) and (10) there follow the relations

$$(26) \qquad \begin{cases} \sigma^*\sigma^* = \textit{identity} \\ \phi^*\sigma^*\phi^*\sigma^* = q^r \times \textit{identity} \end{cases} \quad \textit{in } G.$$

The calculations we are about to make are somewhat more perspicuous in terms of matrices. Let us therefore choose a base $\mathfrak{g}_1, \cdots, \mathfrak{g}_\rho$ for G and put

$$(27) \qquad \begin{cases} \phi^*(\mathfrak{g}_i) = \sum_{j=1}^{\rho} a_{ij}\mathfrak{g}_j \\ \sigma^*(\mathfrak{g}_i) = \sum_{j=1}^{\rho} s_{ij}\mathfrak{g}_j \end{cases} \qquad (i = 1, \cdots, \rho),$$

the a_{ij} and s_{ij} being rational integers. Write $A = (a_{ij})$, $S = (s_{ij})$. The relations (26) then become

$$(28) \qquad \begin{cases} S^2 = I \\ (SA)^2 = q^r I \end{cases} \qquad (I = \rho \times \rho \text{ unit matrix}).$$

From this one concludes easily

$$(28') \qquad (SA^\nu)^2 = q^{r\nu} I \qquad (\nu = 0, 1, 2, \cdots),$$

which is just (4′) in G.

Remark. As mentioned earlier, for curves ($r = 1$) the group $\mathfrak{N}^1(V \times V)$ is finitely generated. If in this case we take for G the entire group $\mathfrak{N}^1(V \times V)$, then our preceding calculations remain valid, except possibly (10), since $\mathfrak{N}^1(V \times V)$ may not possess a base consisting of classes which are rational over K. If it does, however, then from (28) there results $(\det A)^2 = q^\rho$, where ρ is the Picard number of $V^1 \times V^1$. Since A is an integral matrix, ρ must be even if q is an odd power of a prime. *Then whether or not $V^1 \times V^1$ has a base for divisors rational over K_1, it follows that $\rho > 3$ whenever q is an odd power of a prime.*

Resuming the general argument, we wish to consider the characteristic polynomial $f(x)$ of the matrix A. Of course $f(x) = x^\rho + e_1 x^{\rho-1} + \cdots + e_\rho$,

the coefficients e_j being as in (11), (12), (21). We have $f(x)=\det(xI-A)$ $=\det[S(xI-A)S]$, since $(\det S)^2=1$. Hence

$$f(x)=\det(xI-SAS)=\det(xI-q^rA^{-1})$$
$$=(-1)(\det A)^{-1}x^\rho\det((q^r/x)I-A),$$

by (28). Thus

$$f(x)=e_\rho^{-1}x^\rho f(q^r/x). \tag{29}$$

Again let $\alpha_1,\cdots,\alpha_t$ be the distinct roots of (21)—i. e., the distinct roots of $f(x)$. For each α_i the quantity q^r/α_i must also be a root of $f(x)$, by (29).[10] Call it α_{si}, so that $i\to si$ designates a permutation of $1,\cdots,t$ of period 2.

Referring now to the numbers $\beta_1,\cdots,\beta_t$ introduced in (20), (22), it is important to show that $\beta_{si}=\beta_i$ for each i. To prove this, write the diagonal class $\mathfrak{d}_0$ in terms of the base $\mathfrak{g}_1,\cdots,\mathfrak{g}_\rho$. Say $\mathfrak{d}_0=c_1\mathfrak{g}_1+\cdots+c_\rho\mathfrak{g}_\rho$. Since $\sigma^*(\mathfrak{d}_0)=\mathfrak{d}_0$, we have

$$\sum_{i=1}^{\rho}c_is_{ij}=c_j \qquad (j=1,\cdots,\rho). \tag{30}$$

Let the coefficients of A^ν be denoted by $a_{ij}^{(\nu)}$. Then from (9) we obtain

$$N_\nu=\langle\mathfrak{d}_\nu,\mathfrak{d}_0\rangle=\sum_{i,j,k}c_ia_{ij}^{(\nu)}c_k\langle\mathfrak{g}_j,\mathfrak{g}_k\rangle. \tag{31}$$

Since σ is a biregular birational transformation it is clear that

$$N_\nu=\langle\mathfrak{d}_\nu,\mathfrak{d}_0\rangle=\langle\sigma^*(\mathfrak{d}_\nu),\sigma^*(\mathfrak{d}_0)\rangle=\langle\mathfrak{d}'_\nu,\mathfrak{d}_0\rangle,$$

and so

$$N_\nu=\sum c_ia_{ij}^{(\nu)}s_{jk}c_k\langle\mathfrak{g}_h,\mathfrak{g}_k\rangle.$$

From (28′), $A^\nu S=q^{r\nu}SA^{-\nu}$. Therefore the last equation can be written

$$N_\nu=q^{r\nu}\sum c_is_{ij}a_{jk}^{(-\nu)}c_h\langle\mathfrak{g}_h,\mathfrak{g}_k\rangle.$$

Using (30) we obtain

$$N_\nu=q^{r\nu}\sum c_ia_{ij}^{(-\nu)}c_k\langle\mathfrak{g}_j,\mathfrak{g}_k\rangle. \tag{32}$$

Let us now define N_ν for $\nu<0$ by means of the difference equation (12). It is clear that the values so obtained for N_{-1}, N_{-2}, etc. must be the same as the values calculated from (31) by putting $\nu=-1,-2$, etc. Referring to (32) we conclude that

$$N_\nu=q^{r\nu}N_{-\nu} \qquad (\nu=0,1,2,\text{etc.}) \tag{33}$$

Now from (22) we have (for any value of ν)

---

[10] Each α_i is thus an algebraic integer that divides some power of the field characteristic.

$$N_\nu = \sum_{i=1}^{t} \beta_i \alpha_i{}^\nu = \sum \beta_i q^{r\nu}/\alpha_{si}{}^\nu = q^{r\nu} \sum \beta_i \alpha_{si}{}^{-\nu}.$$

From (33),

$$N_\nu = q^{r\nu} \sum \beta_i \alpha_i{}^{-\nu}.$$

Therefore, $\sum(\beta_i - \beta_{si})\alpha_i{}^{-\nu} = 0$ for all ν. Since the α_i are distinct, we conclude that $\beta_i = \beta_{si}$. Now from (20),

$$\Phi(u) = \sum_{i=1}^{t} \beta_i \alpha_i/(1 - \alpha_i u),$$

Hence

$$\begin{aligned}\Phi(1/q^r u) &= \sum \beta_i \alpha_i/(1 - \alpha_i/q^r u) \\ &= \sum \beta_i \alpha_i/(1 - 1/\alpha_{si} u) = -\sum \beta_i \alpha_i \alpha_{si} u/(1 - \alpha_{si} u).\end{aligned}$$

Since $\alpha_i \alpha_{si} = q^r$, $\beta_i = \beta_{si}$, this becomes

$$\begin{aligned}\Phi(1/q^r u) &= -q^r u \sum \beta_i/(1 - \alpha_i u) \\ &= -q^r u^2 \sum \beta_i \alpha_i/(1 - \alpha_i u) - q^r u \sum \beta_i.\end{aligned}$$

From (23) we have $\sum \beta_i = \chi(V)$. Hence

$$\Phi(1/q^r u) = -q^r u^2 \cdot \Phi(u) - q^r u \cdot \chi(V). \tag{34}$$

Let us now assume that the β_i are rational integers, which of course must be the case if $Z(u)$ is a rational function. From (24) and the preceding calculations we derive the functional equation

$$Z(1/q^r u) = (-1)^{\chi(V)} (\prod \alpha_i{}^{\beta_i}) \cdot u^{\chi(V)} Z(u). \tag{35}$$

If no α_i is equal to $q^{r/2}$, then by putting $u = q^{-r/2}$ in (35) we find $\prod \alpha_i{}^{\beta_i} = (-1)^\chi q^{r\chi/2}$ $(\chi = \chi(V))$. Moreover in this case $\chi(V)$ must be even, because the β_i occur in equal pairs. It is easy to see that even if some α_i is equal to $q^{r/2}$, say $\alpha_1 = q^{r/2}$, we must nonetheless have $\prod \alpha_i{}^{\beta_i} = q^{r\chi/2}$, if we continue with our assumption that the β_i are rational integers. For $\alpha_2, \cdots, \alpha_t$ must occur in pairs α_i, α_{si}, and we have $\alpha_i{}^{\beta_i} \alpha_{si}{}^{\beta_{si}} = (\alpha_i \alpha_{si})^{\beta_i} = q^{r\beta_i}$. The assertion follows easily. Hence, if the β_i are integers we obtain the following equation for $Z(u)$:

$$Z(1/q^r u) = (-1)^\chi q^{r\chi/2} u^\chi \cdot Z(u) \qquad (\chi = \chi(V)). \tag{36}$$

This agrees precisely with the form predicted by Weil [11], save that Weil's factor ± 1 is here found to be $(-1)^\chi$.

8. **A sheaf-theoretic formulation.** In the framework of sheaf theory

the foregoing discussion assumes a rather different aspect, of which we shall now give a brief account. Needless to say, the finiteness assumption made in § 5 cannot be circumvented. It takes on here a slight different form, relating to the Chern classes of the sheaves involved. In order to avail ourselves of Serre's sheaf theory we shall now take as ground field the algebraic closure K of the field K_1. All functions are supposed to be rational over K.

Let $\mathcal{O}$ denote the sheaf of local rings on $V \times V$, and let $\mathcal{O}_\nu$ denote the sheaf of local rings of the subvariety Δ_ν, extended by zero to all of $V \times V$. From results of Serre [7, No. 55, Lemme 2, Corollaire] and from standard theorems of homological algebra (Cartan-Eilenberg [1], Proposition 4.3, p. 151; Theorem 6.1′, p. 157) it follows that there exists a *resolution* of $\mathcal{O}_0$ $(=\mathcal{O}_{\Delta_0})$ consisting of locally free sheaves $\mathcal{E}_j$ on $V \times V$ $(j=1,\cdots,r)$ and homomorphisms such that the sequence

$$(37) \qquad 0 \to \mathcal{E}_r \to \mathcal{E}_{r-1} \to \cdots \to \mathcal{E}_1 \to \mathcal{O} \to \mathcal{O}_0 \to 0$$

is exact. In fact, for $j < r$, $\mathcal{E}_j$ can be taken to be a direct sum of locally free sheaves of dimension 1.

Now for any coherent sheaf $\mathcal{F}$ on $V \times V$ we can form the *reciprocal image* sheaf $\mathcal{F}^{(\nu)} = \phi^{-\nu}(\mathcal{F})$ with respect to the regular mapping ϕ^ν. Viz., for any point (u,v) write $\phi^\nu(u,v) = (u',v)$, $u' = u^{q^\nu}$. Then the stalk of $\mathcal{F}^{(\nu)}$ at (u,v) is defined to be $\mathcal{O}_{(u,v)} \otimes_{\phi^\nu} \mathcal{F}_{(u',v)}$, meaning the tensor product over $\mathcal{O}_{(u',v)}$, where $\mathcal{O}_{(u,v)}$ is regarded as $\mathcal{O}_{(u',v)}$-module *via* ϕ^ν. This operation is fully described in [6]. We have $\phi^{-\nu}(\mathcal{O}) = \mathcal{O}$, and it is readily seen that $\mathcal{E}_1 \to \mathcal{O}$ induces a homomorphism $\phi^{-\nu}(\mathcal{E}_1) \to \phi^{-\nu}(\mathcal{O})$, i.e., $\mathcal{E}_1^{(\nu)} \to \mathcal{O}$, with the property that the image of $\mathcal{E}_1^{(\nu)}$ in $\mathcal{O}$ is precisely the sheaf of ideals of the subvariety Δ_ν. Thus by taking reciprocal images of (37) we obtain for each ν a sequence

$$(38) \qquad 0 \to \mathcal{E}_r^{(\nu)} \to \mathcal{E}_{r-1}^{(\nu)} \to \cdots \to \mathcal{E}_1^{(\nu)} \to \mathcal{O} \to \mathcal{O}_\nu \to 0.$$

This sequence is exact. The proof can be outlined as follows (we take $\nu = 1$ for simplicity of notation): At any point (u,u) of Δ_0 we can find generators $\xi_1,\cdots,\xi_r$ for the ideal p of Δ_0 in $\mathcal{O}_{(u,u)}$ which form a subset of a regular system of parameters at (u,u) and which are such that their transforms $\xi_1' = \phi^*(\xi_1),\cdots,\xi_r' = \phi^*(\xi_r)$ by ϕ form a subset of a regular system of parameters at $(u^{1/q},u)$ and generate the ideal p' of Δ_1 in $\mathcal{O}_{(u^{1/q},u)}$. The corresponding Koszul resolutions of p and p' are exact (Cartan-Eilenberg [1], Proposition 4.3, p. 151), and it is readily seen that the reciprocal image operation ϕ^{-1} simply transforms the Koszul resolution of p into the Koszul resolution of p'. Thus we conclude that $\mathrm{Tor}_h(\mathcal{O}, \mathcal{O}_0) = 0$ for $h \geqq 1$, where

again we mean that $\mathcal{O}$ at $(u^{1/q}, u)$ and $\mathcal{O}_0$ at (u, u) are both regarded as $\mathcal{O}_{(u,u)}$-modules, the former by means of ϕ. The exactness of (38) then follows at once from the definition of the torsion functor.

Now from $\mathcal{O}_\nu$ and $\mathcal{O}_0$ form the ordinary tensor product over $\mathcal{O}$ $(\nu > 0)$. At any of the N_ν points on $\Delta_\nu \cap \Delta_0$ the stalk of this sheaf is isomorphic to K, because Δ_ν and Δ_0 are transversal at each point of intersection. Therefore we have

$$N_\nu = \chi(\mathcal{O}_\nu \otimes \mathcal{O}_0) \qquad (\nu = 1, 2, 3, \cdots), \tag{39}$$

where for any coherent sheaf $\mathcal{F}$ on $V \times V$ we understand

$$\chi(\mathcal{F}) = \sum_{m=0}^{\infty} (-1)^m \dim_K H^m(V \times V, \mathcal{F}).$$

We require now the fact that $\operatorname{Tor}_h^{\mathcal{O}}(\mathcal{O}_\nu, \mathcal{O}_0) = 0$ for $h > 0$. This is easily established from the transversality of Δ_ν, Δ_0 by means of a Koszul resolution at any point of intersection. Consequently the tensor product, over $\mathcal{O}$, of the two complexes (37), (38) is an acyclic resolution of $\mathcal{O}_\nu \otimes \mathcal{O}_0$. From the familiar properties of the Euler-Poincaré characteristic we arrive at the formula

$$N_\nu = \sum_{i,j=0}^{r} (-1)^{i+j} \chi(\mathcal{E}_i^{(\nu)} \otimes_{\mathcal{O}} \mathcal{E}_j) \qquad (\nu > 0), \tag{40}$$

where we understand $\mathcal{E}_0^{(\nu)} = \mathcal{E}_0 = \mathcal{O}$. We can then write

$$\Phi(u) = \sum_{\nu=1}^{\infty} N_\nu u^{\nu-1} = \sum_{i,j=1}^{r} \Phi_{ij}(u),$$

where

$$\Phi_{ij}(u) = (-1)^{i+j} \sum_{\nu=1}^{\infty} \chi(V \times V, \mathcal{E}_i^{(\nu)} \otimes_{\mathcal{O}} \mathcal{E}_j) \cdot u^{\nu-1}. \tag{41}$$

Under the assumption of a finite base for numerical equivalence it is possible to prove a general result which yields the rationality of the above functions $\Phi_{ij}(u)$ as a special case: Let X be a non-singular projective variety (over a field of arbitrary characteristic); let $\psi: X \to X$ be a regular mapping of X into itself; and let $\mathcal{F}$, $\mathcal{G}$ be locally free sheaves defined on X. Consider the function

$$\Lambda(u) = \sum_{\nu=1}^{\infty} \chi(X, \mathcal{F}^{(\nu)} \otimes \mathcal{G}) \cdot u^{\nu-1},$$

where $\mathcal{F}^{(\nu)}$ is the reciprocal image of $\mathcal{F}$ with respect to the ν-th iterate ψ^ν of ψ. Then, under the assumption of a finite base, it can be proved that $\Lambda(u)$ is a rational function of u. This follows quickly with the aid of Hirzebruch's

formula for the Euler-Poincaré characteristic of a locally free sheaf.[11] It is probable that appropriate generalizations of Weil's conjectures could be made for $\Lambda(u)$.

Finally, there are some special cases where the rationality of $\Lambda(u)$ depends merely upon the existence of a finite base for numerical equivalence of divisors on X—for example, when either $\mathfrak{F}$ or $\mathfrak{G}$ is the sheaf of cross sections of a vector bundle whose structure group can be reduced to the group of triangular matrices.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton, 1956.

[2] W.-L. Chow, "On equivalence classes of cycles in an algebraic variety," *Annals of Mathematics*, vol. 64 (1956), pp. 450-479.

[3] E. Hecke, *Vorlesungen über die Theorie der Algebraischen Zahlen*, Leipzig, 1923.

[4] F. Hirzebruch, *Neue Topolgische Methoden in der Algebraischen Geometrie*, Ergebnisse der Mathematik, Berlin, 1956.

[5] A. Néron, "Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps," *Bulletin de la Société Mathématique de France*, vol. 80 (1952), pp. 101-106.

[7] J.-P. Serre, "Faisceaux algébriques cohérents," *ibid.*, vol. 61 (1955), pp. 197-288.

[8] A. Weil, *Foundations of Algebraic Geometry*, New York, 1946.

[9] ———, *Variétés Abéliennes et Courbes Algébriques*, Paris, 1948.

[10] ———, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Paris, 1948.

[11] ———, "Numbers of solutions of equations in finite fields," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 497-508.

[12] ———, "Number theory and algebraic geometry," *Proceedings of the International Congress of Mathematicians* (Amsterdam), 1950, pp. 90-100.

[11] See Hirzebruch [4] for characteristic zero; for characteristic p this has been proved by one of the authors (forthcoming article in this Journal) and, independently, by A. Grothendieck (exposition by A. Borel and J.-P. Serre to appear).

ON RAMIFICATION THEORY IN NOETHERIAN RINGS.* [1]

By M. Auslander and D. A. Buchsbaum.

Introduction. The purpose of this paper is to give a fairly general ramification theory for noetherian rings. To illustrate the types of results obtained let us assume that S is a noetherian ring and R is a subring of S such that the kernel $\mathfrak{J}$ of the mapping $\phi : S \otimes_R S \to S$ defined by $\phi(x \otimes y) = xy$ is a finitely generated ideal in $S \otimes_R S$. In § 2 we show that S is an unramified extension of R (see § 1 for definition) if and only if S is a projectice $S \otimes_R S$-module, or equivalently, if and only if $\mathfrak{J}$ is a direct summand of $S \otimes_R S$. From this it follows that if $\mathfrak{H}_{S/R} = \phi(\mathfrak{N})$, where $\mathfrak{N}$ is the annihilator of $\mathfrak{J}$ in $S \otimes S$, then a prime ideal $\mathfrak{P}$ in S is ramified if and only if it contains $\mathfrak{H}_{S/R}$. We call $\mathfrak{H}_{S/R}$ the *homological different* of S over R.

The main object of § 3 is to show that if R is a noetherian integrally closed domain with field of quotients K, L a finite field extension of K and S an integral extension of R in L, then $\mathfrak{H}_{S/R}$ is contained in $\mathfrak{D}_{S/R}$, where $\mathfrak{D}_{S/R}$ is the usual different defined using the trace mapping on L. There are examples which show that $\mathfrak{H}_{S/R} \neq \mathfrak{D}_{S/R}$ in general. However, in the case that S is R-projective, we have that $\mathfrak{H}_{S/R} = \mathfrak{D}_{S/R}$. As an application we prove that if R is a regular local ring of dimension less than or equal to two and L is a separable field extension, then S is unramified over R if and only if each minimal prime ideal is unramified over R. This result has been obtained independently by J.-P. Serre (unpublished) and has been used by M. Nagata to prove the theorem in general i. e. for regular local rings of arbitrary dimension [7].

§ 4 is devoted to showing that under various conditions if S is unramified over R, then S is R-projective. For instance, this is the case if R is a noetherian, integrally closed domain and S is an integral extension of R in a finite, separable field extension of the field of quotients of R.

§ 5 is devoted to certain homological considerations and is the only place in the paper where any homology theory is used. Perhaps the most striking result obtained here is that if S is unramified over R and R-projective and T

---

* Received October 20, 1958.

[1] This work was done with the partial support of NSF Grants G-5864 and G-4232.

is a regular ring of finite Krull dimension (i.e. T is a noetherian ring and every local ring of T is a regular local ring) containing R, then $S \otimes_R T$ is regular if it is noetherian.

It has recently been brought to our attention that E. Noether had considered the ideals $\mathcal{J}$, $\mathfrak{N}$ and $\mathfrak{H}_{S/R}$ from a somewhat different point of view in [5].

1. Notation and terminology. All rings to be considered in this paper will be assumed commutative with identity element and all modules will be unitary. A ring S together with a ring homomorphism $f\colon R \to S$ such that $f(1) = 1$ will be called an *R-algebra.* Ideals in S will be denoted by capital German letters and ideals in R by lower case German letters. If $\mathfrak{A}$ is an ideal in S, then we call the ideal $f^{-1}(\mathfrak{A})$ in R the *contraction of* $\mathfrak{A}$ and denote it by $\mathfrak{A} \cap R$. We shall consider $R/\mathfrak{A} \cap R$ to be a subring of $S/\mathfrak{A}$, the identification being given by the monomorphism induced by f. If $x \in R$, then we denote $f(x)$ in S by x, provided there is no danger of confusion. Thus if $\mathfrak{a}$ is an ideal in R, we shall denote the ideal $S \cdot f(\mathfrak{a})$ by $S \cdot \mathfrak{a}$. It is clear that $(S \cdot \mathfrak{a}) \cap R$ contains $\mathfrak{a}$.

A subset U of a ring is called a *multiplicative* system if a) whenever u_1 and u_2 are in U, the product $u_1 u_2$ is in U, and b) 0 is not in U; 1 is in U. The only multiplicative systems in R that we shall consider are those that do not meet the kernel of f. Suppose U is a multiplicative system in R and U' is a multiplicative system in S containing U (i.e. U' contains $f(U)$). Then $f\colon R \to S$ induces a homomorphism $f'\colon R_U \to S_{U'}$ which makes $S_{U'}$ an R_U-algebra. In particular, if $\mathfrak{P}$ is a prime ideal in S and $\mathfrak{p} = \mathfrak{P} \cap R$, then $S_{\mathfrak{P}}$ is an $R_{\mathfrak{p}}$-algebra and $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is a subfield of $S_{\mathfrak{P}}/\mathfrak{P}S_{\mathfrak{P}}$.

We define the R-algebra S^e to be the ring $S \otimes_R S$ with the mapping of R into S^e being given by $r \to r \otimes 1$. S^e is called the enveloping algebra of the R-algebra S. The map $\phi\colon S^e \to S$ defined by $\phi(x \otimes y) = xy$ is an R-algebra epimorphism. Thus all S-modules may be considered as S^e-modules. The kernel of ϕ will be denoted by $\mathcal{J}$ which is the ideal generated by $\{1 \otimes x - x \otimes 1\}$, and the annihilator of $\mathcal{J}$ will be denoted by $\mathfrak{N}$. If U is a multiplicative system, we denote by $U \otimes U$ the multiplicative system in S^e consisting of all elements of the form $u_1 \otimes u_2$ where u_1, u_2 are in U. The map $(S_U)^e \to (S^e)_{U \otimes U}$ defined by $x/u_1 \otimes y/u_2 \to x \otimes y/u_1 \otimes u_2$ is an R-algebra isomorphism which we shall use to identify these algebras. If E is an S-module, then $E_U = E_{U \otimes U}$. Finally, if V is a multiplicative system in R such that V is contained in U, then $S_U \otimes_R S_U = S_U \otimes_{R_V} S_U$.

A prime ideal $\mathfrak{P}$ in the R-algebra S is said to be *unramified* if $\mathfrak{p} = R \cap \mathfrak{P}$ has the following properties:

a) $\mathfrak{p}S_{\mathfrak{P}} = \mathfrak{P}S_{\mathfrak{P}}$;

b) $S_{\mathfrak{P}}/\mathfrak{p}S_{\mathfrak{P}}$ is a separable field extension of $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.[2]

The R-algebra S is said to be *unramified* if

a) every prime ideal in S is unramified;

b) for each prime ideal $\mathfrak{p}$ in R there are only a finite number of prime ideals $\mathfrak{P}$ in S such that $\mathfrak{p} = \mathfrak{P} \cap R$.

In other words, S is unramified if and only if given any prime ideal $\mathfrak{p}$ in R which is the contraction of a prime ideal in S and $U = R - \mathfrak{p}$, then $S_U/\mathfrak{p}S_U$ is a separable $R_U/\mathfrak{p}R_U$-algebra.

2. Ramification criteria.

LEMMA 2.1. *If S is an R-algebra, the following statements are equivalent:*

a) *S is S^e-projective;*

b) *the exact sequence $0 \to \mathcal{J} \to S^e \xrightarrow{\phi} S \to 0$ splits;*

c) *there is an element z in S^e such that $z(1 \otimes x) = z(x \otimes 1)$ for all $x \in S$, and $\phi(z) = 1$;*

d) $\phi(\mathcal{N}) = S$.

Further, if R is a field, then S is S^e-projective if and only if S is a separable R-algebra.

Proof. Clearly a) implies b). If b) holds, there is an S^e-homomorphism $p: S \to S^e$ such that ϕp is the identity. Let $z = p(1)$. It is easy to see that z is the desired element to make c) hold, so b) implies c).

Now suppose that c) is true. Then z is in $\mathcal{N}$ so that $\phi(\mathcal{N})$ contains $\phi(z) = 1$. Hence $\phi(\mathcal{N}) = S$. Thus c) implies d).

If d) holds, there is a z in $\mathcal{N}$ such that $\phi(z) = 1$. Define $p: S \to S^e$ by $p(s) = sz$. Since z is in $\mathcal{N}$, p is an S^e-homomorphism so that b) holds. Clearly b) implies a) so that d) implies a).

The last statement in the theorem is found in [6, Theorem 1].

PROPOSITION 2.2. *If the R-algebra S is S^e-projective, then S is unramified.*

---

[2] If R is a field, an R-algebra S is said to be *separable* if S is a finite-dimensional R-algebra which is a direct sum of separable field extensions of R.

Proof. We must show that if $\mathfrak{p}$ is any prime ideal in R where $\mathfrak{p} = \mathfrak{P} \cap R$ for some prime $\mathfrak{p} \subset S$ and $U = R - \mathfrak{p}$, then $S_U/\mathfrak{p}S_U$ is a separable $R_U/\mathfrak{p}R_U$-algebra. Since $R_U/\mathfrak{p}R_U$ is a field, we need only show that $S_U/\mathfrak{p}S_U$ is $S_U/\mathfrak{p}S_U \otimes S_U/\mathfrak{p}S_U$-projective, where the tensor product is taken over $R_U/\mathfrak{p}R_U$.

Since S is S^e-projective, there is a z in S^e such that $\phi(z) = 1$ and $z(x \otimes 1) = z(1 \otimes x)$ for all $x \in S$. We also have the commutative diagram

$$\begin{array}{ccccc}
S \otimes_R S & \xrightarrow{f} & S_U \otimes_{R_U} S_U & \xrightarrow{g} & S_U/\mathfrak{p}S_U \otimes_{R_U} S_U/\mathfrak{p}S_U \\
\phi \downarrow & & \phi' \downarrow & & \phi'' \downarrow \\
S & \longrightarrow & S_U & \longrightarrow & S_U/\mathfrak{p}S_U
\end{array}$$

where the maps are the obvious ones. Let $z'' = gf(z)$. Then it is clear that $\phi''(z'') = 1$ and that z'' is in the annihilator of the kernel of ϕ''. But since $S_U/\mathfrak{p}S_U \otimes_{R_U} S_U/\mathfrak{p}S_U = S_U/\mathfrak{p}S_U \otimes_F S_U/\mathfrak{p}S_U$ (where $F = R_U/\mathfrak{p}R_U$) we have by 2.1 that S is unramified.

PROPOSITION 2.3. *Let R be an integral domain with field of quotients K. If S is an R-algebra such that S is S^e-projective, then $S \otimes_R K$ is a separable K-algebra. In particular, if S is an integral domain, then its field of quotients is a separable field extension of K.*

Proof. It is easy to see that condition c) of 2.1 holds for the K-algebra $S \otimes_R K$ since it holds for S. If S is an integral domain, then $S \otimes_R K$ is also and is therefore the field of quotients of S. Hence the second part of the proposition is true.

PROPOSITION 2.4. *Let S be a noetherian ring which is an R-algebra such that every maximal ideal in S is unramified. Then any R-derivation D of S into a finitely generated S-module E is zero.*

Proof. Let $\mathfrak{M}$ be a maximal ideal of S and $\mathfrak{m} = \mathfrak{M} \cap R$. Denote by $E_{\mathfrak{M}}$ the $S_{\mathfrak{M}}$-module $E \otimes_S S_{\mathfrak{M}}$ and by $D_{\mathfrak{M}}\colon S_{\mathfrak{M}} \to E_{\mathfrak{M}}$ the derivation induced by $D\colon S \to E$.

Since $\mathfrak{M}$ is unramified, we have $\mathfrak{m}S_{\mathfrak{M}} = \mathfrak{M}S_{\mathfrak{M}}$. Since D is a derivation over R, $D_{\mathfrak{M}}$ is a derivation over $R_{\mathfrak{m}}$ so that $D_{\mathfrak{M}}(\mathfrak{m}S_{\mathfrak{M}})$ is contained in $\mathfrak{m}E_{\mathfrak{M}} = \mathfrak{M}E_{\mathfrak{M}}$. Therefore $D_{\mathfrak{M}}$ induces a derivation

$$\bar{D}_{\mathfrak{M}}\colon S_{\mathfrak{M}}/\mathfrak{M}S_{\mathfrak{M}} \to E_{\mathfrak{M}}/\mathfrak{M}E_{\mathfrak{M}}$$

over $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$. But since $\mathfrak{M}$ is unramified, $S_{\mathfrak{M}}/\mathfrak{M}S_{\mathfrak{M}}$ is a separable extension of $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$ so that $\bar{D}_{\mathfrak{M}} = 0$. Hence $D_{\mathfrak{M}}(S_{\mathfrak{M}})$ is contained in $\mathfrak{M}E_{\mathfrak{M}}$.

Iterating this argument, we have that $D_{\mathfrak{M}}(S_{\mathfrak{M}})$ is contained in $\cap \mathfrak{M}^i E_{\mathfrak{M}} = 0$ so that $D_{\mathfrak{M}} = 0$.

Since $D_{\mathfrak{M}} = 0$ for every maximal ideal $\mathfrak{M}$ of S, it follows easily that $D = 0$.

THEOREM 2.5. *Let S be a noetherian R-algebra such that $\mathfrak{J}$ is a finitely generated ideal in S^e. Then the following statements are equivalent:*

a) *S is S^e-projective;*

b) *S is unramified;*

c) *Every maximal ideal in S is unramified;*

d) *Every R-derivation of S into a finitely generated S-module is zero.*

Proof. We have already shown in 2.2 that a) implies b) and clearly b) implies c). Proposition 2.4 shows that c) implies d). Hence we need only prove that d) implies a).

To show that S is S^e-projective, it suffices to show that the exact sequence

$$0 \to \mathfrak{J} \to S^e \to S \to 0 \tag{1}$$

splits.

Observe first that for any S-module E, $\mathrm{Hom}_S(\mathfrak{J}/\mathfrak{J}^2, E)$ is isomorphic to the group of R-derivations of S into E. Letting $E = \mathfrak{J}/\mathfrak{J}^2 = S \otimes_{S^e} \mathfrak{J}$, and observing that $\mathfrak{J}/\mathfrak{J}^2$ is a finitely generated S-module (since $\mathfrak{J}$ is assumed to be finitely S^e-generated), we have $\mathrm{Hom}_S(\mathfrak{J}/\mathfrak{J}^2, \mathfrak{J}/\mathfrak{J}^2) = 0$ and hence $\mathfrak{J}/\mathfrak{J}^2 = 0$, i.e. $\mathfrak{J} = \mathfrak{J}^2$. Since $\mathfrak{J}$ is finitely generated, there is a y_0 in $\mathfrak{J}$ such that $x = y_0 x$ for each $x \in \mathfrak{J}$.

Now define a map $p \colon S^e \to \mathfrak{J}$ by letting $p(1) = y_0$. Then for all $x \in \mathfrak{J}$, we have $p(x) = xp(1) = xy_0 = x$. Thus the sequence (1) above splits and we are done.

LEMMA 2.6. *Let S be a ring, E a finitely generated S-module, and $\mathfrak{A}$ the annihilator of E. If U is a multiplicative system in S, then the annihilator in S_U of E_U is $\mathfrak{A}_U$.*

Proof. It is obvious that $\mathfrak{A}_U$ is contained in the annihilator of E_U. Suppose, then, that $(s/u)E_U = 0$. Let E be generated by $e_1, \cdots, e_n$. Then E_U is also generated by $e_1, \cdots, e_n$ and we have $(s/u)e_i = 0$ for $i = 1, \cdots, n$. But then there is a u' in U such that $u'se_i = 0$ for $i = 1, \cdots, n$ so that $u's$ is in $\mathfrak{A}$. Hence s is in $\mathfrak{A}_U$ and so is s/u.

We now define the *homological different* of the R-algebra S to be the ideal $\phi(\mathfrak{N})$ in S, and denote it by $\mathfrak{H}_{S/R}$.

THEOREM 2.7. *Let S be a noetherian R-algebra such that $\mathfrak{J}$ in S^e is a finitely generated ideal. A prime ideal $\mathfrak{P}$ in S is unramified if and only if $\mathfrak{P}$ does not contain $\mathfrak{H}_{S/R}$.*

Proof. Let $\mathfrak{P}$ be a prime ideal in S, $\mathfrak{p}=\mathfrak{P}\cap R$, $U=S-\mathfrak{P}$, $V=R-\mathfrak{p}$. Then S_U is an R_V-algebra, $(S^e)_{U\otimes U}=S_U\otimes_R S_U=S_U\otimes_{R_V}S_U$, the kernel of map $\bar\phi\colon S^e{}_U\to S_U$ is $\mathfrak{J}_{U\otimes U}$, and $\mathfrak{N}_{U\otimes U}$ is the annihilator of $\mathfrak{J}_{U\otimes U}$. Moreover, S_U is a noetherian R_V-algebra and $\mathfrak{J}_{U\otimes U}$ is a finitely generated ideal in $(S_U)^e$.

Suppose $\mathfrak{P}$ does not contain $\mathfrak{H}_{S/R}$. Then $(\mathfrak{H}_{S/R})_U=S_U=\bar\phi(\mathfrak{N}_{U\otimes U})$ and so, by 2.1, S_U is $(S_U)^e$-projective. But then, by 2.5, S_U is an unramified R-algebra. It is thus easy to see that $\mathfrak{P}$ is unramified.

Now suppose that $\mathfrak{P}$ is unramified. Then $\mathfrak{P}S_U$ is unramified over R_V and again by 2.5 (since $\mathfrak{P}S_U$ is the only maximal ideal in S_U), S_U is $(S_U)^e$-projective. Thus by 2.1, $\bar\phi(\mathfrak{N}_{U\otimes U})=S_U$. Since $\bar\phi(\mathfrak{N}_{U\otimes U})=(\mathfrak{H}_{S/R})_U$, we have $(\mathfrak{H}_{S/R})_U=S_U$ which implies that $\mathfrak{P}$ does not contain $\mathfrak{H}_{S/R}$.

COROLLARY 2.8. *Let R be an integral domain with field of quotients K. If S is a noetherian R-algebra such that $\mathfrak{J}$ is a finitely generated ideal in S^c, and $S\otimes_R K$ is not a separable K-algebra, then every prime ideal in S is ramified.*

LEMMA 2.9. *If S is a noetherian ring, and E is a finitely generated S-module, then $\bigcap_{\mathfrak{M}}(\bigcap_i \mathfrak{M}^i E)=0$, where $\mathfrak{M}$ runs through all maximal ideals of S.*

Proof. Let e be an element of $\bigcap_{\mathfrak{M}}(\bigcap_i \mathfrak{M}^i E)$, and let $\mathfrak{A}$ be the annihilator of e. If $e\neq 0$, then $\mathfrak{A}$ is a proper ideal of S and so is contained in some maximal ideal $\mathfrak{M}$. Since e is in $\bigcap \mathfrak{M}^i E$, there is an m in $\mathfrak{M}$ such that $(1-m)e=0$. However, $(1-m)$ is not in $\mathfrak{A}$ so that e must be zero.

PROPOSITION 2.10. *Let S be a noetherian R-algebra, and $\mathfrak{J}$ finitely generated in S^e. Then S is unramified if and only if for every maximal ideal $\mathfrak{M}$ of S every R-derivation $D\colon S\to S/\mathfrak{M}$ is zero.*

Proof. Proposition 2.4 shows us that if S is unramified then every R-derivation $D\colon S\to S/\mathfrak{M}$ is zero. To prove the converse, it is sufficient (by 2.5) to show that every R-derivation $D\colon S\to E$ is zero, where E is any finitely generated S-module.

If $D\colon S\to E$ is an R-derivation, E finitely generated, and $\mathfrak{M}$ a maximal ideal of S, then $E/\mathfrak{M}E$ is a finite-dimensional vector space over $S/\mathfrak{M}$ and so the derivation $\bar D\colon S\to E/\mathfrak{M}E$ is zero, where $\bar D$ is the composition

$S \xrightarrow{D} E \to E/\mathfrak{M}E$. Therefore $D(S)$ is contained in $\mathfrak{M}E$. Iterating this (i.e. observing that $\mathfrak{M}^iE/\mathfrak{M}^{i+1}E$ is a finite-dimensional vector space over $S/\mathfrak{M}$) we see that $D(S)$ is contained in $\bigcap \mathfrak{M}^iE$. Since this is so for all maximal ideals $\mathfrak{M}$ of S, we have $D(S)$ is contained in $\bigcap_{\mathfrak{M}} (\bigcap_i \mathfrak{M}^iE) = 0$ (by 2.9). Hence $D = 0$.

PROPOSITION 2.11. *Let S and T be R-algebras such that $\mathfrak{J} = \operatorname{Ker} (S^e \xrightarrow{\phi} S)$ is finitely generated in S^e and S is noetherian. If S is unramified, then $S \otimes_R T$ is unramified as a T-algebra. If, further, T is unramified, then $S \otimes_R T$ is unramified as an R-algebra.*

Proof. Since S is unramified, we have by 2.5 that the exact sequence

$$0 \to \mathfrak{J} \to S^e \to S \to 0$$

splits. Therefore the sequence

$$0 \to \mathfrak{J} \otimes_R T \to S^e \otimes_R T \to S \otimes_R T \to 0$$

is exact and splits. But $S^e \otimes_R T = (S \otimes_R T) \otimes_T (S \otimes_R T) = (S \otimes_R T)^e$ as a T-algebra. Hence $S \otimes_R T$ is $(S \otimes_R T)^e$-projective. Thus, by 2.2, it follows that $S \otimes_T T$ is an unramified T-algebra.

If, in addition, T is an unramified R-algebra, then it easily follows from the fact that $S \otimes_R T$ is an unramified T-algebra, that $S \otimes_R T$ is an unramified R-algebra.

3. The homological different and different. Throughout this section, R will be an integral domain with field of quotients K, L a finite-dimensional K-algebra, and S a subring of L containing R such that $S \otimes_R K = L$. We shall denote $\operatorname{Hom}_R(S, R)$ by S^* and $\operatorname{Hom}_K(L, K)$ by L^*.

We define the map $\tau: S \otimes_R S \to \operatorname{Hom}_R(S^*, S)$ to be $\tau(x \otimes y)(f) = xf(y)$ for f in S^*. By [3; VI, 5.2] if S is a projective and finitely generated R-module, then τ is an isomorphism. In particular, $\sigma: L \otimes_K L \to \operatorname{Hom}_K(L^*, L)$ which is similarly defined, is an isomorphism.

Since $S \otimes_R K = L$, every element of S^* is uniquely extendable to an element of L^*. If S^* generates all of L^* over K, then we have a natural map $\rho: \operatorname{Hom}_R(S^*, S) \to \operatorname{Hom}_K(L^*, L)$. We therefore obtain the following diagram which is easily shown to be commutative:

$$\begin{tikzcd}
 & \mathrm{Hom}_S(S^*,S) \arrow[r] \arrow[d] & \mathrm{Hom}_L(L^*,L) \arrow[d] & \\
S\otimes_R S \arrow[r, "\tau"] \arrow[d, "\phi"'] & \mathrm{Hom}_R(S^*,S) \arrow[r, "\rho"] & \mathrm{Hom}_K(L^*,L) \arrow[r, "\sigma^{-1}"] & L\otimes_K L \arrow[d, "\phi'"] \\
S \arrow[rrr] & & & L.
\end{tikzcd}$$

If f is in $\mathrm{Hom}_L(L^*,L)$, it can be seen by standard techniques of linear algebra that $\phi'\sigma^{-1}(f)=f(\mathrm{Tr})$, where $\mathrm{Tr}\colon L\to K$ is the trace map.

An explicit description of ρ and of $\phi'\sigma^{-1}\rho$ can be given as follows: let $v^1,\cdots,v^n$ be elements of S^* which form a basis for L^* over K. Then for f in $\mathrm{Hom}_R(S^*,S)$ we have $\rho(f)$ defined by $\rho(f)(v^i)=f(v^i)$. If we let $v_1,\cdots,v_n$ be the basis of L over K dual to $v^1,\cdots,v^n$ and set $v_i=u_i/r_0$ with u_i in S, r_0 in R (using the fact that $S\otimes_R K=L$), we can easily see that every element s of S can be written $s=\sum r_iv_i$ with r_i in R and that $\mathrm{Tr}(r_0S)$ is contained in R. Thus if we let $T'\colon S\to R$ be the restriction of $r_0\mathrm{Tr}$ to S, we have for f in $\mathrm{Hom}_S(S^*,S)$ that $\phi'\sigma^{-1}\rho(f)=(1/r_0)f(T')$. If $\mathrm{Tr}(S)$ were contained in R (e.g. if S were integral over R) then $\phi'\sigma^{-1}\rho(f)=f(\mathrm{Tr}')$ where Tr' is the restriction of Tr to S.

We now define the *complementary module*, $\mathfrak{C}_{S/R}$, and the *different*, $\mathfrak{D}_{S/R}$, as follows:

$$\mathfrak{C}_{S/R}=\{x \text{ in } L/\mathrm{Tr}(xS) \text{ is contained in } R\}$$

$$\mathfrak{D}_{S/R}=\{x \text{ in } L/x\mathfrak{C}_{S/R} \text{ is contained in } S\}.$$

From the above remarks, we can see that $\phi'\sigma^{-1}\rho(\mathrm{Hom}_S(S^*,S))$ is contained in $\mathfrak{D}_{S/R}$. For suppose x is in $\mathfrak{C}_{S/R}$ and f is in $\mathrm{Hom}_S(S^*,S)$. Then $x[(1/r_0)f(T')]=x(\rho(f)(\mathrm{Tr}))=\rho(f)(\mathrm{Tr}\circ x)$, where $\mathrm{Tr}\circ x\colon L\to K$ is defined by $\mathrm{Tr}\circ x(y)=\mathrm{Tr}(xy)$ for y in L. Since $\mathrm{Tr}\circ x$ restricted to S maps S into R, $\rho(f)(\mathrm{Tr}\circ x)$ is in S. Therefore $x\cdot\phi'\sigma^{-1}\rho(f)$ is in S for all x in $\mathfrak{C}_{S/R}$.

Now let us make $\mathrm{Hom}_R(S^*,S)$ an S^e-module by defining $(x\otimes y)f(g)=x\cdot f(g\circ y)$ for x, y in S, f in $\mathrm{Hom}_R(S^*,S)$, g in S^*. Then τ is an S^e-homomorphism. Furthermore, $\mathrm{Hom}_S(S^*,S)$ is equal to the set of all f in $\mathrm{Hom}_R(S^*,S)$ such that $\mathcal{J}f=0$. Thus, since $\mathcal{N}=$ annihilator of $\mathcal{J}$ in S^e, we have $\tau(\mathcal{N})$ is contained in $\mathrm{Hom}_S(S^*,S)$.

We can go even a little further. Let

$$\mathcal{W}=\mathrm{Ker}(S\otimes_R S\to L\otimes_K L=S\otimes_R S\otimes_R K),$$

and let $\mathcal{A}$ in S^e be the annihilator of $\mathcal{J}/\mathcal{W}$ ($\mathcal{W}$ is obviously contained in $\mathcal{J}$).

Since $\mathfrak{W}$ is the torsion submodule of S^e (as an R-module), and since S is torsion-free as an R-module, $\tau(w)=0$ for all w in $\mathfrak{W}$. Thus, if a is in $\mathfrak{A}$, we have $a\mathfrak{J}$ is contained in $\mathfrak{W}$ and $0=\tau(a\mathfrak{J})=\tau(a)\mathfrak{J}$. Thus by the remark above $\tau(a)$ is in $\mathrm{Hom}_S(S^*,S)$ which implies that $\tau(\mathfrak{A})$ is contained in $\mathrm{Hom}_S(S^*,S)$.

Combining all the above remarks, and resorting to the commutative diagram above, we have shown

PROPOSITION 3.1. *Let R be an integral domain with field of quotients K, L a finite-dimensional K-algebra, and S a subring of L containing R such that $S\otimes_R K=L$ and $S^*\otimes_R K=L^*$. Then if $\mathfrak{A}$ is the annihilator of $\mathfrak{J}/\mathfrak{W}$, $\phi(\mathfrak{A})$ is contained in $\mathfrak{D}_{S/R}$. In particular, $\mathfrak{H}_{S/R}$ is contained in $\mathfrak{D}_{S/R}$.*

PROPOSITION 3.2. *Let R, K, L and S be as in* 3.1 *and in addition assume L is a field. Then L is a separable extension of K if and only if $\mathfrak{H}_{S/R}\neq 0$ (i.e. $\mathfrak{N}$ is not contained in $\mathfrak{J}$).*

Proof. If L is not separable, the trace map is identically zero, so that for all f in $\mathrm{Hom}_S(S^*,S)$, $\rho(f)(\mathrm{Tr})=0$. Since $\mathfrak{H}_{S/R}=\phi(\mathfrak{N})=\phi'\sigma^{-1}\rho\tau(\mathfrak{N})$ and $\tau(\mathfrak{N})$ is contained in $\mathrm{Hom}_S(S^*,S)$, we have $\mathfrak{H}_{S/R}=0$.

If L is separable, the exact sequence

$$0\to\mathfrak{J}'\to L\otimes_K L\to L\to 0$$

splits. However, $L=S\otimes_R K$, $L\otimes_K L=S^e\otimes_R K$, and $\mathfrak{J}'=\mathfrak{J}\otimes_R K$. Thus the annihilator $\mathfrak{N}'$ of $\mathfrak{J}'$ is $\mathfrak{N}\otimes_R K$ (by 2.6), and $\mathfrak{N}'$ is not contained in $\mathfrak{J}'$. Therefore $\mathfrak{N}$ is not contained in $\mathfrak{J}$ and $\mathfrak{H}_{S/R}\neq 0$.

PROPOSITION 3.3. *Let R be an integrally closed integral domain with field of quotients K, L a separable K-algebra, and S a subring of L containing R which is integral over R and such that $S\otimes_R K=L$. Then* $\mathrm{Hom}_S(S^*,S)$ *is isomorphic to $\mathfrak{D}_{S/R}$ under the map $f\to f(\mathrm{Tr})$. If S is a projective, finitely generated R-module, then $\mathfrak{H}_{S/R}=\mathfrak{D}_{S/R}$.*

Proof. Since L is a separable K-algebra, the map $L\to L^*$ given by $x\to\mathrm{Tr}\circ x$ is an isomorphism. Under this isomorphism, $\mathfrak{C}_{S/R}$ is mapped onto S^*. Thus $\mathrm{Hom}_S(S^*,S)\approx\mathrm{Hom}_S(\mathfrak{C}_{S/R},S)$ and this latter module is isomorphic to $\mathfrak{D}_{S/R}$. The composite isomorphism is the one described above, namely $f\to f(\mathrm{Tr})$ (Tr is here restricted to S). Furthermore, by standard arguments, it is easy to see that $S^*\otimes_R K=L^*$ so that all our previous discussion (including commutative diagram) holds. Moreover, if S is finitely generated over R and R-projective, then τ is an isomorphism, $\mathfrak{W}=0$, and $\tau(\mathfrak{N})=\mathrm{Hom}_S(S^*,S)$. Thus in this case $\mathfrak{H}_{S/R}=\mathfrak{D}_{S/R}$.

Throughout the rest of this section we shall denote the R-module $\mathrm{Hom}_R(E, R)$ by E^*, where E is an arbitrary R-module.

PROPOSITION 3.4. *Let R be a noetherian domain such that every proper principal ideal is unmixed (e.g. R is integrally closed). Let A be a finitely generated R-module such that $A = A^{**}$, and B a finitely generated torsion-free R-module containing A such that B/A is a non-trivial torsion module. Then $\mathfrak{a}(B/A)$ is unmixed of rank one ($\mathfrak{a}(B/A)$ is the annihilator of B/A in R).*[3]

Proof. Let $b_1, \cdots, b_t$ be generators of B. Then $\mathfrak{a}(B/A) = \{r \text{ in } R/rb_i$ is in A for $i = 1, \cdots, t\} = \cap\, \mathfrak{a}_i$, where $\mathfrak{a}_i = \{r \text{ in } R/rb_i \text{ is in } A\}$. Thus if each $\mathfrak{a}_i$ is unmixed of rank one, then so is $\mathfrak{a}(B/A)$. We may therefore suppose that $B = A + Rb$, b not in A, and B/A is a torsion module.

Observe next that if h is in A^*, then h can be extended to a map $\bar{h}: A \otimes_R K \to K$. Moreover, if x in $A \otimes_R K$ is such that $\bar{h}(x) = 0$ for all h in A^*, then $x = 0$. As a result, we have that r is in $\mathfrak{a}(B/A)$ if and only if $r\bar{h}(b) = \bar{h}(rb)$ is in R for all h in A^*. For if r is in $\mathfrak{a}(B/A)$, then rb is in A so that $\bar{h}(rb) = h(rb)$ is in R. Conversely, if $\bar{h}(rb)$ is in R for all h in A^*, then the map $A^* \to R$ given by $h \to \bar{h}(rb)$ is an element of $A^{**} = A$ so that $\bar{h}(rb) = h(a_0)$ for some a_0 in A and all h in A^*. Thus $\bar{h}(rb - a_0) = 0$ for all h in A^* and by the above remarks, $rb = a_0$ i.e. r is in $\mathfrak{a}(B/A)$.

Since A^* is finitely generated, say by $h_1, \cdots, h_n$, we see that $\mathfrak{a}(B/A) = \{r \text{ in } R/\bar{h}_i(rb)$ is in R for $i = 1, \cdots, n\}$. Let $\bar{h}_i(b) = u_i/v$. Then r is in $\mathfrak{a}(B/A)$ if and only if r is in $\cap\,(v) : u_i$ i.e. $\mathfrak{a}(B/A) = \cap\,(v) : u_i$. Now by assumption on R, (v) is an unmixed ideal of rank one so that $(v) : u_i$ is also. Thus $\mathfrak{a}(B/A)$ is unmixed of rank one.

COROLLARY 3.5. *Let R be an integrally closed noetherian integral domain with field of quotients K, L a separable field extension of K, and S the integral closure of R in L. Then if $\mathfrak{D}_{S/R} \neq S$, $\mathfrak{D}_{S/R}$ must be of rank one.*

This follows from 3.4 by letting $R = A = S$ and $B = \mathfrak{C}_{S/R}$ and observing that $\mathfrak{D}_{S/R} = \mathfrak{a}(\mathfrak{C}_{S/R}/S)$.

PROPOSITION 3.6. *With R, K, L and S as above, we have $\mathfrak{D}_{S/R} = S$ if and only if every minimal prime ideal of S is unramified.*

Proof. By 2.7, every minimal prime ideal of S is unramified if and only if rank $\mathfrak{H}_{S/R}$ is greater than one. Since $\mathfrak{D}_{S/R}$ contains $\mathfrak{H}_{S/R}$, we have that if every minimal prime is unramified, then $\mathfrak{D}_{S/R}$ has rank greater than one. Thus, by 3.5, $\mathfrak{D}_{S/R} = S$.

[3] We would like to thank O. Goldman for suggesting this proposition to us.

Conversely, let $\mathfrak{D}_{S/R}=S$, $\mathfrak{P}$ be a minimal prime of S, and $\mathfrak{p}=\mathfrak{P}\cap R$. Then $\mathfrak{p}$ is a minimal prime of R and $R_{\mathfrak{p}}$ is a regular local ring of dimension one. Since $S_{\mathfrak{p}}$ is a finitely generated, torsion-free $R_{\mathfrak{p}}$-module, $S_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-free. We have by 3.3 that $\mathfrak{H}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}=\mathfrak{D}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}$. But it is easily seen that $\mathfrak{H}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}=\mathfrak{H}_{S/R}\otimes_S S_{\mathfrak{p}}$ and $\mathfrak{D}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}=\mathfrak{D}_{S/R}\otimes_S S_{\mathfrak{p}}$. Therefore $\mathfrak{H}_{S_{\mathfrak{p}}/R_{\mathfrak{p}}}=S_{\mathfrak{p}}$ and thus $\mathfrak{P}$ is unramified.

COROLLARY 3.7. *Let R, K, S and L be as in 3.5 and assume further that S is R-projective. Then S is unramified if and only if every minimal prime ideal of S is unramified.*

Proof. Since S is R-projective and finitely generated, we have $\mathfrak{H}_{S/R}=\mathfrak{D}_{S/R}$. Furthermore, S is unramified if and only if $\mathfrak{H}_{S/R}=S$ (by 2.5). Thus 3.6 implies 3.7.

The following theorem has also been obtained independently by Serre.

THEOREM 3.8. *Let R be a regular local ring of dimension less than or equal to two, and let K, S, and L be as above. Then S is unramified if and only if every minimal prime ideal of S is unramified.*

Proof. We need only show that S is R-projective, for then we may apply 3.7. However, by [2, 2.10] it is sufficient to show that S is a Macaulay ring (S is semi-local). Since $\dim S\leqq 2$, and since S is integrally closed, we have that every principal ideal of S is unmixed and that every ideal of rank two that is generated by two elements is unmixed. Hence S is Macaulay and therefore R-projective.

4. On being free.

Throughout this section, R will be an integrally closed local domain with maximal ideal $\mathfrak{m}$ and field of quotients K. The residue class field $R/\mathfrak{m}$ will be denoted by F.

PROPOSITION 4.1. *Let L be a separable K-algebra and S an integral extension of R in L such that $S\otimes_R K=L$ and is unramified. Then $\mathfrak{D}_{S/R}=S$.*

Proof. Since S is unramified, $\mathfrak{H}_{S/R}=S$. However, since $\mathfrak{H}_{S/R}$ is contained in $\mathfrak{D}_{S/R}$, we have $\mathfrak{D}_{S/R}=S$.

LEMMA 4.2. *Let S be an R-algebra containing R which is torsion-free over R and such that*

a) *S is finitely generated over R,*

b) *there is an element t in $S/\mathfrak{m}S$ such that $S/\mathfrak{m}S=F[t]$.*

If θ in S is such that $\theta\to t$ under the natural map $S\to S/\mathfrak{m}S$, then

$S=R[\theta]$ and $\{1,\theta,\cdots,\theta^{n-1}\}$ is a free basis for S over R (where $n=[S/\mathfrak{m}S:F]$).

Proof. Since $S/\mathfrak{m}S=F[t]$, we have that $\{1,t,\cdots,t^{n-1}\}$ is a basis for $S/\mathfrak{m}S$ over F. Since R is a local ring, this implies that $\{1,\theta,\cdots,\theta^{n-1}\}$ generates S over R and is a minimal generating set for S over R. Also, since R is integrally closed, we know that the minimal polynomial f in $K[x]$ for θ has its coefficients in R. We will show that degree $f=n$, hence that $\{1,\theta,\cdots,\theta^{n-1}\}$ is a basis for $K[\theta]$ over K. This will imply that $\{1,\theta,\cdots,\theta^{n-1}\}$ is a free basis for S over R.

Let $\bar{f}$ in $F[X]$ be the corresponding polynomial of f. Then $\bar{f}(t)=0$ so that $\deg\bar{f}\geqq n$. On the other hand, since θ^n is in S, we have $\theta^n=\sum_{i=0}^{n-1}r_i\theta^i$, r_i in R. Therefore $\deg f\leqq n$ and we are done.

PROPOSITION 4.3. *Let S be a torsion-free R-algebra containing R which is unramified and finitely generated over R. Then S is a free R-module on n generators (where $n=[S/\mathfrak{m}S:F]$). Moreover, if L is the full ring of quotients of S, $[L:K]=n$ and S is integrally closed in L.*

Proof. Let us assume first that F is an infinite field. Then it is well known [4] that $S/\mathfrak{m}S=F[t]$. Thus, by 4.2, we have that S is R-free with basis $\{1,\theta,\cdots,\theta^{n-1}\}$.

Now suppose F is finite. Let X be an indeterminate, and consider the local domain $R[X]_{\mathfrak{m}^*}=R'$, where $\mathfrak{m}^*$ is the extension of $\mathfrak{m}$ to $R[X]$. The maximal ideal $\mathfrak{m}'$ of R' is $R'\mathfrak{m}^*$ and $R'/\mathfrak{m}'=F'=F(X)$. R' is integrally closed since $R[X]$ is and rings of quotients of integrally closed rings are integrally closed.

We now have R' contained in S', where $S'=S[X]_{\mathfrak{m}^*}$, S' a finitely generated torsion-free R'-module, and $[S'/\mathfrak{m}'S':F']=n$. If we show that S' is unramified over R', and use the fact that F' is infinite, we will have that S' is a free R'-module on n generators. This will imply that S is R-free on n generators for if $s_1,\cdots,s_m$ is a minimal generating set for S over R, it is also one for S' over R', hence a free basis for S' over R' and therefore a free basis for S over R, with $m=n$.

Since S is unramified, S is S^e-projective so that the exact sequence

$$0\to\mathfrak{J}\to S^e\to S\to 0$$

splits. Therefore, the exact sequence

$$0\to\mathfrak{J}\otimes_R R'\to S^e\otimes_R R'\to S\otimes_R R'\to 0$$

splits. Since $S' = S[X] \otimes_{R[X]} R' = S \otimes_R (R[X] \otimes_{R[X]} R') = S \otimes_R R'$ and $(S')^e = S' \otimes_{R'} S' = S^e \otimes_R R'$, we see that S' is $(S')^e$-projective and therefore S' is unramified over R'. This then shows that S is R-free on n generators. The rest of the proposition follows from standard arguments [4].

THEOREM 4.4. *Let R be a noetherian integral domain (not necessarily local) with field of quotients K, and L a separable K-algebra. If S is an unramified integral extension of R in L such that $S \otimes_R K = L$, then S is R-projective.*

Proof. By standard localization arguments, this result follows from 4.3.

PROPOSITION 4.5. *Let S be a local ring containing R which is unramified and finitely generated over R. Then S is R-free.*

Proof. Since S is unramified, $S \otimes_R K$ is a separable K-algebra. Let $S' = \operatorname{Im}(S \to S \otimes_R K)$. Then S' is torsion-free and finitely generated over R, and we have the exact sequence

(E) $$0 \to t(S) \to S \to S' \to 0,$$

where $t(S)$ is the R-torsion submodule of S, and is finitely generated over R. If we can show that $t(S)/\mathfrak{m}t(S) = 0$, we will have $t(S) = 0$. Therefore $S \approx S'$ and so S will be torsion-free, hence free (by 4.3). Since S is unramified, $S/\mathfrak{m}S$ is a field and therefore the map $S/\mathfrak{m}S \to S'/\mathfrak{m}S'$, being an epimorphism, must be an isomorphism. Moreover, $S/\mathfrak{m}S$ is a separable extension of F so that $S'/\mathfrak{m}S'$ is also. Hence S' is unramified (by 2.5 it is sufficient to test ramification of S' by its unique maximal ideal) and by 4.3 is free over R. Therefore the sequence (E) splits over R so that the sequence

$$0 \to t(S)/\mathfrak{m}t(S) \to S/\mathfrak{m}S \to S'/\mathfrak{m}S' \to 0$$

is exact. Since $S/\mathfrak{m}S \approx S'/\mathfrak{m}S'$, we have $t(S)/\mathfrak{m}t(S) = 0$, hence $t(S) = 0$ and $S \approx S'$.

PROPOSITION 4.6. *Let R be analytically normal (i.e. $\hat{R}$, the completion of R, is also an integrally closed local domain) and let S be a ring containing R which is unramified and finitely generated over R. Then S is R-free.*

Proof. $S\mathfrak{m}$ is the radical of S, so that $\hat{S}$ contains $\hat{R}$ and $\hat{S}$ is a finitely generated $\hat{R}$-module. Now $\hat{S} = S_1 + \cdots + S_n$ (direct sum), where each S_i is a local ring which is an $\hat{R}$-algebra. In fact, each S_i contains a copy of $\hat{R}$. It can also be easily seen that each S_i is an unramified $\hat{R}$-algebra (since $\hat{S}$ is unramified over R). Therefore, by 4.5, each S_i is free over $\hat{R}$, which implies

that $\hat{S}$ is R-free. Since S is finitely generated over R, $\hat{S}$ being R-free implies that S is R-free [1, Theorem 3.2].

Since an integrally closed geometric local ring is analytically normal, we see that an unramified integral, finitely generated extension ring S of an integrally closed geometric local ring R is R-free. Hence if R is a normal affine ring (not necessarily local), S is R-projective.

LEMMA 4.7. *Let R be a noetherian ring (not necessarily an integrally closed local domain) and let S be a ring containing R which is finitely generated as an R-module. If S is R-projective, then R is a direct summand of S as an R-module.*

Proof. From the exact sequence

$$0 \to R \to S \to S/R \to 0$$

it is clearly sufficient to prove that S/R is R-projective. Let $\mathfrak{m}$ be a maximal ideal of R. Then the exact sequence

$$0 \to R_{\mathfrak{m}} \to S_{\mathfrak{m}} \to (S/R)_{\mathfrak{m}} \to 0$$

splits since $S_{\mathfrak{m}}$ is a projective (hence free) $R_{\mathfrak{m}}$-module, and 1 is part of a free basis for $S_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$. Therefore $(S/R)_{\mathfrak{m}}$ is free for every maximal ideal $\mathfrak{m}$ and so by [3, VII, Exercise 11] S/R is R-projective.

PROPOSITION 4.8. *Let $R \subset S \subset T$ be noetherian rings with T a finitely generated projective unramified R-algebra. Then S is unramified over R if and only if T is S-projective.*

Proof. Suppose T is S-projective. Then we have the commutative diagram

$$\begin{array}{ccc} S \otimes_R S & \longrightarrow & T \otimes_R T \\ \downarrow & & \downarrow \\ S & \longrightarrow & T. \end{array}$$

Since T is S-projective, $T \otimes_R T$ is $S \otimes_R S$-projective, and S is a direct summand of T as an S- hence also as an $S \otimes_R S$-module. But T is $T \otimes_R T$-projective since T is an unramified R-algebra. Hence S is $S \otimes_R S$-projective.

By [3, IX, Proposition 2.3] (letting $\Lambda = \Gamma = S$, $A = S$, $\Sigma = R$, $B = T$) we have that since S is $S \otimes_R S$-projective (being unramified) and T is R-projective, then T is S-projective.

5. Ramification and homology.

PROPOSITION 5.1. *Let S and T be R-algebras such that S is R-projective and S is S^e-projective. If E is an $S \otimes_R T$-module, then* $\mathrm{hd}_{S\otimes_R T} E = \mathrm{hd}_T E$ *and thus* $\mathrm{gl.\,dim}\, S \otimes_R T \leqq \mathrm{gl.\,dim}\, T$.

Further, if S is R-free, then $\mathrm{gl.\,dim}\, S \otimes_R T = \mathrm{gl.\,dim}\, T$.

Proof. By [3; XVI, sec. 4] we have the spectral sequence

$$H^p(S, \mathrm{Ext}^q{}_T(E, C)) \underset{p}{\Longrightarrow} \mathrm{Ext}^n{}_{S\otimes_R T}(E, C),$$

where C is an $S \otimes_R T$-module. Since S is S^e-projective, this spectral sequence collapses to $H^0(S, \mathrm{Ext}^n{}_T(E, C)) \approx \mathrm{Ext}^n{}_{S\otimes_R T}(E, C)$. From the fact that C is an arbitrary $S \otimes_R T$-module, it follows that $\mathrm{hd}_{S\otimes_R T} E \leqq \mathrm{hd}_T E$.

But considering $S \otimes_R T$ as a T-algebra, we have by [3; XVI, Exercise 5] that

$$\mathrm{hd}_T E \leqq \mathrm{hd}_T S \otimes_R T + \mathrm{hd}_{S\otimes_R T} E.$$

Since S is R-projective, it follows that $S \otimes_R T$ is T-projective. Therefore $\mathrm{hd}_T S \otimes_R T = 0$ and thus $\mathrm{hd}_T E \leqq \mathrm{hd}_{S\otimes_R T} E$, which gives the desired equality.

From the fact that $\mathrm{hd}_{S\otimes_R T} E = \mathrm{hd}_T E$ for arbitrary $S \otimes_R T$-modules E it follows that $\mathrm{gl.\,dim}\, S \otimes_R T \leqq \mathrm{gl.\,dim}\, T$. Further, if S is R-free and A is a T-module, then $\mathrm{hd}_T A = \mathrm{hd}_T S \otimes_R A$ since $S \otimes_R E$ is a direct sum of copies of A. But $\mathrm{hd}_T S \otimes_R A = \mathrm{hd}_{S\otimes_R T} S \otimes_R A$ by the previous arguments. Thus $\mathrm{hd}_T A = \mathrm{hd}_T S \otimes_R A$, which means that $\mathrm{gl.\,dim}\, T \leqq \mathrm{gl.\,dim}\, S \otimes_R T$.

COROLLARY 5.2. *Let S and T be noetherian R-algebras such that S is unramified and R-projective and $\mathfrak{J}$ is a finitely generated ideal in S^e. If T is a regular ring of finite (Krull) dimension and $S \otimes_R T$ is noetherian, then $S \otimes_R T$ is a regular ring of (Krull) dimension less than or equal to that of T.*

Further, if S is R-free (e.g. R a local ring) then the dimensions of $S \otimes_R T$ and T are equal.

Proof. By 2.5 we have that S is S^e-projective. Since T is a regular ring of finite dimension, we have by [1, Corollary 4.8] that $\mathrm{gl.\,dim}\, T < \infty$. Therefore it follows from 5.1 that $\mathrm{gl.\,dim}\, S \otimes_R T \leqq \mathrm{gl.\,dim}\, T$, which means that $S \otimes_R T$ is a regular ring of dimension less than or equal to that of T. The rest of the corollary follows from the fact that if $\mathrm{gl.\,dim}\, S \otimes_R T = \mathrm{gl.\,dim}\, T$, then the dimensions of $S \otimes_R T$ and T are equal.

PROPOSITION 5.3. *Let S be an R-algebra, where R is an integral domain*

with field of quotients K such that S^e is noetherian and $0 < [S \otimes_R K : K] < \infty$. Then $\mathrm{hd}_{S \otimes_R S} S = 0$ *or* ∞.

Proof. First we observe that $\mathrm{hd}_{S^e} S \geqq \mathrm{hd}_{L^e} L$ where $L = S \otimes K$ and $L^e = (S \otimes_R K) \otimes_K (S \otimes_R K)$. Since $[L : K] < \infty$, it is well known that if L is not a separable K-algebra, then $\mathrm{hd}_{L^e} L = \infty$. Thus we may assume that L is a separable K-algebra. Further, let us assume that S is not S^e-projective. Therefore we have that $\mathfrak{J} \neq (0)$ and the ideal generated by $\mathfrak{J}$ and $\mathfrak{N}$ is not S^e. By 2.6 we know that $\mathfrak{N} \otimes_R K$ is the annihilator of the kernel of $L^e \to L$. From the fact that L is a separable K-algebra we know that $\mathrm{hd}_{L^e} L = 0$ and hence by 2.1 $\mathfrak{N} \otimes_R K \neq (0)$. Therefore $\mathfrak{N} \neq (0)$ and thus $\mathfrak{J}$ consists entirely of zero divisors in S^e.

Let $\mathfrak{M}$ be a maximal ideal in S^e containing $\mathfrak{J}$ and $\mathfrak{N}$. Then the ideal $\mathfrak{J}_{\mathfrak{M}}$ in the local ring $S^e{}_{\mathfrak{M}}$ is not zero and consists entirely of zero-divisors. Therefore we conclude from the exact sequence

$$0 \to \mathfrak{J}_{\mathfrak{M}} \to (S^e)_{\mathfrak{M}} \to S_{\mathfrak{M}} \to 0$$

that the annihilator of $S_{\mathfrak{M}}$ as an $(S^e)_{\mathfrak{M}}$-module is not zero and consists entirely of zero-divisors. Hence by [2, 6.2] we have that the $\mathrm{hd}_{(S^e)_{\mathfrak{M}}} S_{\mathfrak{M}} = \infty$. Since $\mathrm{hd}_{S^e} S \geqq \mathrm{hd}_{(S^e)_{\mathfrak{M}}} S_{\mathfrak{M}}$, we have that $\mathrm{hd}_{S^e} S = \infty$.

Appendix.

PROPOSITION A.1. *Let R be a noetherian ring and T an R-algebra which is a finitely generated module. If S_1 and S_2 are unramified subalgebras of T, then the subalgebra generated by S_1 and S_2 is an unramified R-algebra. Thus T contains an unramified R-algebra, which contains all the unramified R-subalgebras of T.*

Proof. By 2.11 we know that $S_1 \otimes_R S_2$ is an unramified R-algebra. Therefore $Im(S_1 \otimes S_2 \to T)$ is an unramified R-subalgebra of T, which establishes the first part of the proposition. The second part follows from the chain conditions in T.

We next observe that Proposition 4.5 is true without assuming that S is a local ring. As in the proof of Proposition 4.5, it suffices to show that $t(S)$, the torsion submodule of S, is zero.

Since S is unramified, $S \otimes_R K$ is a separable K-algebra. Let $S' = Im(S \to S \otimes K)$. Then S' is a torsion-free R-algebra which is unramified since it is the image of an unramified R-algebra. Since $t(S)$ is a finitely

generated R-torsion module, there is a non-zero x in R such that $xt(S) = 0$. Now let $\mathfrak{M}$ be a maximal ideal in S. Then $t(S) \subset \mathfrak{M}$ for if not, we have that $S_{\mathfrak{M}}$ and $t(S)_{\mathfrak{M}} = x(S_{\mathfrak{M}}) = 0$ which is impossible.

Since S' is R-projective, we have that

$$0 \to t(S)/\mathfrak{m}t(S) \to S/\mathfrak{m}S \to S'/\mathfrak{m}S' \to 0$$

is exact. Thus

$$0 \to (t(S)/\mathfrak{m}t(S))_{\mathfrak{M}} \to (S'/\mathfrak{m}S)_{\mathfrak{M}} \to (S'/\mathfrak{m}S')_{\mathfrak{M}} \to 0$$

is exact. Since both S and S' are unramified, the map $(S/\mathfrak{m}S)_{\mathfrak{M}} \to (S'/\mathfrak{m}S')_{\mathfrak{M}} \to 0$ is a field epimorphism, hence an isomorphism. Thus $(t(S)/\mathfrak{m}t(S))_{\mathfrak{M}} = 0$ for all maximal ideals $\mathfrak{M}$ of S which implies that $t(S)/\mathfrak{m}t(S) = 0$. Hence $t(S) = 0$, which means that $S \approx S'$ and thus we are done.

PROPOSITION A. 2. *Let $R \subset S \subset T$ be noetherian, integrally closed domains such that T is a finitely generated R-module. Then T is unramified over R if and only if T is unramified over S and S is unramified over R.*

Proof. Suppose T is unramified over R. Then T is unramified over S. Since S is integrally closed we know by Proposition 4. 6, that T is S-projective. Thus the result follows from Proposition 4. 8.

REFERENCES.

[1] M. Auslander and D. A. Buchsbaum, "Homological dimension in local rings," *Transactions of the American Mathematical Society*, vol. 82 (1956), pp. 390-405.

[2] ———, "Codimension and multiplicity," *Annals of Mathematics*, vol. 68 (1958), pp. 625-657.

[3] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton, 1956.

[4] W. Krull, "Beiträge zur Arithmetik kommutativer Integritätsbereiche VI," *Mathematische Zeitschrift*, vol. 45 (1939), pp. 1-19.

[5] E. Noether, "Idealdifferentiation und differente, *Journal für die reine und angewandte Mathematik*, vol. 188 (1950), pp. 1-21.

[6] A. Rosenberg and D. Zelinsky, "Cohomology of infinite algebras," *Transactions of the American Mathematical Society*, vol. 82 (1956), pp. 85-98.

[7] M. Nagata, "On purity of the branch locus," *Illinois Journal of Mathematics* (to appear).

ON THE 14-TH PROBLEM OF HILBERT.*[1]

To Professor Oscar Zariski on his sixtieth birthday.

By MASAYOSHI NAGATA.

The following problem is known as the 14-th problem of Hilbert:

Let k be a field and let $x_1, \cdots, x_n$ be algebraically independent elements over k. Let K be a subfield of $k(x_1, \cdots, x_n)$ containing k. Is $k[x_1, \cdots, x_n] \cap K$ finitely generated over k?

The purpose of the present paper is to answer the question in the negative by giving a counter-example. In fact, we shall give a counter-example to the following restricted case, which was the original question of Hilbert, and which we shall call the *original 14-th problem:*

Let G be a subgroup of the full linear group of $k[x_1, \cdots, x_n]$ and let $\mathfrak{o}$ be the set of elements of $k[x_1, \cdots, x_n]$ which are invariant under G. Is $\mathfrak{o}$ finitely generated over k?

We shall note that the construction of our example is *independent of the characteristic* (and k may be the field of complex numbers).

In § 1, we shall pass in review the history of the 14-th problem of Hilbert and shall state remaining problems concerning it. In § 2, we shall construct a counter-example and in § 3, we shall prove a lemma on plane curves which we need for the construction of our counter-example.

1. The history. The 14-th problem of Hilbert is one of the problems offered by Hilbert at the International Congress in Paris (1900) and published in *Archiv f. Math. u. Phys.* (1901) (see [1]).

It seems to the writer that no contribution to the problem was made until 1953 when Zariski proved that the answer of the 14-th problem of Hilbert is affirmative if $\dim K \leqq 2$ (under the notation stated in the introduction). Zariski proved, in fact, a more general result that the following problem, which we shall call the *generalized 14-th problem,* has affirmative answer if $\dim K \leqq 2$:

* Received January 5, 1959.

[1] The work was supported by a research grant of the National Science Foundation.

Let $\mathfrak{o}$ be a normal affine ring over a field k and let K be a subfield of the function field of $\mathfrak{o}$ containing k. Is $\mathfrak{o} \cap K$ an affine ring? (See [2].)

In 1956, the writer gave another proof of the result of Zariski stated above, including the case where $\mathfrak{o}$ is a normal affine ring over a ground ring (see [3]).

In 1957, Rees gave a counter-example to the generalized 14-th problem in the case where $\dim K = 3$. But, the field of quotients of $\mathfrak{o} \cap K$ in his example contains the function field of a non-singular cubic curve (on a projective plane) and therefore his example cannot be a counter-example to the 14-th problem of Hilbert. (See [4].)

In 1958, the writer found at first a counter-example to the 14-th problem and then another example which is a counter-example to the original 14-th problem. This second example was announced at the International Congress in Edinburgh (1958) (see [5]). Though the first example is in the case where $\dim K = 4$, in the second example $\dim K$ is equal to 13. Then the writer noticed that the first example is also a counter-example to the original 14-th problem (and the example will be stated in the present paper).

By virtue of our example, the following two problems will be the remaining problems concerning the 14-th problem of Hilbert:

PROBLEM 1. *Let $\mathfrak{o}$ be a normal affine ring over a ground field k and let G be a group of automorphisms of $\mathfrak{o}$ over k. Find good sufficient conditions for the pair $\mathfrak{o}$ and G so that the set of elements of $\mathfrak{o}$ which are invariant under G forms an affine ring over k.*

PROBLEM 2. *In the 14-th problem of Hilbert, assume that $\dim K = 3$. What is the answer in this case?*

2. The construction of the example. Let $P_1, \cdots, P_r$ be independent generic points of the projective plane S over the prime field π of an arbitrary characteristic. We choose r so that the following is true:

(*) *If a curve C of degree d goes through every P_i with multiplicity at least m (> 0), then d/m is greater than $\sqrt{r}$.*

The existence of such an r will be proved in § 3.

The above assumption implies the following (cf. [5]):

Let $\mathfrak{p}_i$ be the homogeneous prime ideal of P_i in a homogeneous coordinate ring $\mathfrak{H} = k[x, y, z]$ of S over a ground field k, over which the P_i are rational. Set $\mathfrak{a}_m = \cap\, \mathfrak{p}_i^m$ for every natural number m. Then

LEMMA 1. *For any natural number m, there exists a natural number n such that $\mathfrak{a}_m^n \neq \mathfrak{a}_{mn}$.*

Proof. Since the virtual dimension of the system of plane curves of degree d which go through every P_i with multiplicity at least m is equal to $(d^2+3d-rm^2-rm)/2$, we see that $\lim_{m\to\infty} \deg \mathfrak{a}_m/m \leqq \sqrt{r}$.[2] By the assumption (*), we have $\lim \deg \mathfrak{a}_m/m = r$. Since $\deg \mathfrak{a}_m/m > \sqrt{r}$, we see that for a sufficiently large n, $\deg \mathfrak{a}_{mn} \neq \deg \mathfrak{a}_m{}^n$ $(= n\cdot \deg \mathfrak{a}_m)$, which proves the lemma.

Now we shall construct the example. Let a_{ij} $(i=1,2,3;\ j=1,\cdots,r)$ be algebraically independent elements over the prime field and let k be a field containing all the a_{ij}. Then the points $P_i=(a_{i1},a_{i2},a_{i3})$ are independent generic points of the projective plane S over π and they are rational over k. Let $x_1,\cdots,x_r$, $y_1,\cdots,y_r$ be algebraically independent elements over k. Let V^* be the vector space of dimension r over k and let V be the subspace of V^* of dimension $r-3$ which is orthogonal to the vectors $(a_{i1},\cdots,a_{ir})$ $(i=1,2,3)$. Let G be the set of linear transformations σ of $k[x_1,\cdots,x_r, y_1,\cdots,y_r]$ such that i) $\sigma(y_i)=c_iy_i$ with $c_i\in k$ such that $c_1\cdots c_r=1$ and ii) $\sigma(x_i)=c_i(x_i+b_iy_i)$ with $(b_1,\cdots,b_r)\in V$ (and with the same c_i as in i)). Then

THEOREM. *The set* $\mathfrak{o}$ *of elements of* $k[x_1,\cdots,x_r,y_1,\cdots,y_r]$ *which are invariant under* G *is not finitely generated over* k.

Set $t=y_1\cdots y_r$, $u_i=t/y_i$, $v_i=x_iu_i$ and $w_j=\sum a_{ji}v_i$. We shall show at first the following

LEMMA 2. $\mathfrak{o}=k[x_1,\cdots,x_r,y_1,\cdots,y_r]\cap k(w_1,w_2,w_3,t)$.

Proof. It is sufficient to prove that the invariant subfield of $k(x_1,\cdots,x_r, y_1,\cdots,y_r)$ under G is $k(w_1,w_2,w_3,t)$. Let σ be an arbitrary element of G; let c_i and b_i be as above for this σ. $\sigma(t)=c_1\cdots c_rt=t$, hence t is invariant under G. $\sigma(w_j)=\sum a_{ji}(c_ix_i+c_ib_iy_i)t/c_iy_i=w_j+\sum a_{ji}b_it=w_j$, hence $k(w_1,w_2,w_3,t)$ is contained in the invariant subfield. Since a_{ij} are independent over π, $k(x_1,\cdots,x_r,y_1,\cdots,y_r)=k(w_1,w_2,w_3,x_4,\cdots,x_r,y_1,\cdots,y_r)$ and G is a group of linear transformation of $k[w_1,w_2,w_3,x_4,\cdots,x_r,y_1,\cdots,y_r]$: $\sigma(w_j)=w_j$, $\sigma(y_i)=c_iy_i$ with $c_i\in k$ such that $c_1\cdots c_r=1$ and $\sigma(x_i)=c_i(x_i+b_iy_i)$ (for $i\geqq 4$) with $b_i\in k$. Let G' be the set of σ in G which have c_i all equal to 1. Then we see that the invariant subfield for G' is $k(w_1,w_2,w_3,y_1,\cdots,y_r)$. G operates on $k[w_1,w_2,w_3,y_1,\cdots,y_r]$ as the group of linear transformations σ of the following type: $\sigma(w_j)=w_j$ and $\sigma(y_i)=c_iy_i$ with $c_i\in k$ such that $c_1\cdots c_r=1$. Since $t=y_1\cdots y_r$,

---

[2] $\deg \mathfrak{a}_m$ denotes the minimum of $\deg f$ $(f\in\mathfrak{a}_m)$.

$$k(w_1, w_2, w_3, t, y_2, \cdots, y_r) = k(w_1, w_2, w_3, y_1, \cdots, y_r)$$

and G operates on $k[w_1, w_2, w_3, t, y_2, \cdots, y_r]$ as the set G^* of linear transformations σ of the following type: $\sigma(w_j) = w_j$, $\sigma(t) = t$, $\sigma(y_i) = c_i y_i$ with arbitrary non-zero element c_i in k for $i \geqq 2$ and we see that the invariant subfield for G^*, hence for G too, is $k(w_1, w_2, w_3, t)$, which proves the lemma.

Since w_1, w_2, w_3 are algebraically independent over k, we can regard $k[w_1, w_2, w_3]$ as a homogeneous coordinate ring of the projective plane S, setting $x = w_1$, $y = w_2$, $z = w_3$. Then, using the notations at the beginning of this section,

LEMMA 3. *$\mathfrak{o}$ is the set of elements of the form $\sum a_n t^{-n}$ (finite sum) such that* i) *$a_n \in \mathfrak{H}$ and* ii) *if $n > 0$, then $a_n \in \mathfrak{a}_n$.*

Proof. Since a_{ij} are independent over π, we have $k[v_1, \cdots, v_r] = k[w_1, w_2, w_3, v_4, \cdots, v_r]$, which shows that

$$\begin{aligned} &k[x_1, \cdots, x_r, y_1, \cdots, y_r, 1/y_1, \cdots, 1/y_r] \\ &\qquad = k[w_1, w_2, w_3, x_4, \cdots, x_r, y_1, \cdots, y_r, 1/y_1, \cdots, 1/y_r]. \end{aligned}$$

The intersection of this last ring with $k(w_1, w_2, w_3, y_1, \cdots, y_r)$ is equal to $k[w_1, w_2, w_3, y_1, \cdots, y_r, 1/y_1, \cdots, 1/y_r]$. The intersection of this last ring with $k(w_1, w_2, w_3, t)$ is equal to $k[w_1, w_2, w_3, t, 1/t]$. Hence, by virtue of Lemma 2, we see that $\mathfrak{o}$ is contained in $k[w_1, w_2, w_3, t, 1/t]$. Since $\mathfrak{H} = k[w_1, w_2, w_3]$, we have

(1) *Any element of $\mathfrak{o}$ can be expressed in the form $\sum a_n t^{-n}$ (finite sum) with $a_n \in \mathfrak{H}$.*

Let $\mathfrak{v}_i$ be the valuation ring $k[x_1, \cdots, x_r, y_1, \cdots, y_r]_{(y_i)}$ and let V_i be the normalized valuation defined by $\mathfrak{v}_i$. Then $\mathfrak{o}$ is contained in every $\mathfrak{v}_i$.

(2) *An element f of $\mathfrak{H}$ has value not less than m (>0) under V_i if and only if $f \in \mathfrak{p}_i^m$ $(= \mathfrak{p}_i^{(m)})$.*

Proof. $\mathfrak{p}_i$ is generated by $z_i = a_{3i}w_1 - a_{1i}w_3$ and $z'_i = a_{3i}w_2 - a_{2i}w_3$. Obviously $V_i(z_i) = V_i(z'_i) = 1$. Furthermore, we see easily that z_i/t and z'_i/t are algebraically independent modulo the maximal ideal $\mathfrak{m}_i$ of $\mathfrak{v}_i$ over $k(w_3 \text{ modulo } \mathfrak{m}_i)$. Therefore z_i/z'_i modulo $\mathfrak{m}_i$ is transcendental over $k(w_3$ modulo $\mathfrak{m}_i)$. Hence $\mathfrak{H}[z_i/z'_i]_{\mathfrak{n}_i}$ $(\mathfrak{n}_i = \mathfrak{m}_i \cap \mathfrak{H}[z_i/z'_i])$ is a valuation ring dominated by $\mathfrak{v}_i$. Therefore (2) is proved easily.

Furthermore, by the algebraic independence of z_i/t and z'_i/t modulo $\mathfrak{m}_i$ stated above, we have

(3) *If $a_n \in \mathfrak{H}$, then $V_i(\sum a_n t^{-n}) = \min V_i(a_n t^{-n})$, provided that the summation is a finite sum.*

Now we shall prove Lemma 3. If $a_n \in \mathfrak{a}_n$, then a_n is divisible by t^n in $k[x_1, \cdots, x_r, y_1, \cdots, y_r]$ and therefore any element of the form $\Sigma\, a_n t^{-n}$ (finite sum), with $a_n \in \mathfrak{H}$ such that if $n > 0$ then $a_n \in \mathfrak{a}_n$, is in $\mathfrak{o}$. Conversely, if c is an element of $\mathfrak{o}$, then $c = \Sigma\, a_n t^{-n}$ (finite sum) with $a_n \in \mathfrak{H}$ by (1) above. Since $\mathfrak{o}$ is contained in every $\mathfrak{v}_i$, $V_i(c) \geqq 0$ for any i. Therefore, by (2) and (3), we see that if $n > 0$ then $a_n \in \mathfrak{a}_n$. Thus Lemma 3 is proved.

By virtue of Lemmas 1 and 3, in order to prove Theorem, it is sufficient to prove the following

LEMMA 4. *Let $\mathfrak{b}_1, \mathfrak{b}_2, \cdots$ be a sequence of ideals in an integral domain $\mathfrak{S}$ such that* (i) *$\mathfrak{b}_{i+1} \subseteq \mathfrak{b}_i$ and* (ii) *$\mathfrak{b}_i \mathfrak{b}_j \subseteq \mathfrak{b}_{i+j}$. Let t be a transcendental element over $\mathfrak{S}$. Then the set $\mathfrak{S}'$ of elements of the form $\Sigma\, b_j t^{-j}$ (finite sum) with $b_j \in \mathfrak{S}$ such that if $j > 0$ then $b_j \in \mathfrak{b}_j$ forms an integral domain. If $\mathfrak{S}'$ is finitely generated over $\mathfrak{S}$, then there exists an integer m such that $\mathfrak{b}_m{}^l = \mathfrak{b}_{ml}$ for every natural number l.*[3]

Proof. It is obvious that $\mathfrak{S}'$ is an integral domain. Assume that $\mathfrak{S}'$ is finitely generated over $\mathfrak{S}$. Then there exists an s such that $\mathfrak{S}'$ is generated by t and elements of the form $b_i t^{-i}$ with $0 < i \leqq s$, $b_i \in \mathfrak{b}_i$. Let n be an arbitrary natural number. Since, for any element $b_n \in \mathfrak{b}_n$, $b_n t^{-n}$ is in $\mathfrak{S}'$, we have $\mathfrak{b}_n \subseteq \Sigma\, \mathfrak{b}_1{}^{\sigma_1} \cdots \mathfrak{b}_s{}^{\sigma_s}$ where the summation runs over all such that $\Sigma\, \sigma_j \cdot j = n$. Set $s' = s\,!$ and $s'' = ss'$. We consider the case where $n \geqq s''$. Since $\Sigma\, \sigma_j \cdot j = n \geqq s''$, there exists a j such that $\sigma_j \cdot j \geqq s'$. Then $\mathfrak{b}_1{}^{\sigma_1} \cdots \mathfrak{b}_s{}^{\sigma_s} = \mathfrak{b}_j{}^{(s'/j)} \cdot \mathfrak{b}_1{}^{\sigma_1} \cdots \mathfrak{b}_{j-1}{}^{\sigma_{j-1}} \cdot \mathfrak{b}_j{}^{\sigma_j - (s'/j)} \cdot \mathfrak{b}_{j+1}{}^{\sigma_{j+1}} \cdots \mathfrak{b}_s{}^{\sigma_s} \subseteq \mathfrak{b}_{s'} \mathfrak{b}_{n-s'}$. It follows that $\mathfrak{b}_n \subseteq \mathfrak{b}_{s'} \mathfrak{b}_{n-s'}$ and therefore

If $n \geqq s''$, then $\mathfrak{b}_n = \mathfrak{b}_{s'} \mathfrak{b}_{n-s'}$.

Now we consider the case where n is an arbitrary multiple of s'': $n = s''l$. Then the above result shows that $\mathfrak{b}_{s''l} = \mathfrak{b}_{s'}{}^{s(l-1)} \mathfrak{b}_{s''}$. Hence $\mathfrak{b}_{s''l} \subseteq \mathfrak{b}_{s''}{}^l$, whence $\mathfrak{b}_{s''l} = \mathfrak{b}_{s''}{}^l$. This proves Lemma 4 with $m = s''$.

Remark. We can prove Theorem without proving Lemma 4, by the same method as in [5].

3. The existence of r.

PROPOSITION. *If r is the square of a natural number s not less than 4, then r satisfies the requirement in* § 1.

Proof. (i) The case where r is odd. Set $s' = (s+1)/2$ and let C_s, $C_{s'}$, $C'_{s'}$ be independent generic curves of degree s, s', s' respectively. Let $P_1, \cdots, P_s$

[3] This lemma was substantially proved by Rees [4].

be s points among $C_{s'} \cdot C'_{s'}$. Then the P_i are independent generic points of the projective plane over $\pi(C_s)$. Let $P^*_1, \cdots, P^*_s$ be independent generic points of C_s over $\pi(C_s)$, let $C^*_{s'}$ and $C^{*\prime}_{s'}$ be most general curves of degree s' going through the P^*_i, and let $Q^*_1, \cdots, Q^*_{r-s}$ be such that

$$C^*_{s'} \cdot C_s = \Sigma P^*_i + \Sigma_1{}^{(r-s)/2} Q^*_i, \quad C^{*\prime}_{s'} \cdot C_s = \Sigma P^*_i + \Sigma_{(r-s+2)/2}{}^{r-s} Q^*_i.$$

We consider a specialization

$$(P_1, \cdots, P_s, C_{s'}, C'_{s'}) \to (P^*_1, \cdots, P^*_s, C^*_{s'}, C^{*\prime}_{s'})$$

over $\pi(C_s)$. We take $Q_1, \cdots, Q_{r-s}$ so that (1) $\Sigma_1{}^{(r-s)/2} Q_i \subseteq C_{s'} \cdot C_s$, $\Sigma_{(r-s+2)/2}{}^{r-s} Q_i \subseteq C'_{s'} \cdot C_s$ and (2) the Q_i are specialized to the Q^*_i by the specialization considered above.

Assume now that for an m there exists a curve of degree sm which goes through each of given r $(= s^2)$ independent generic points of the projective plane S with multiplicity at least m. Then we see that there exists a curve E of degree sm which goes through the Q_i and the P_i with multiplicity at least m. Assume that E does not contain $C_{s'}$ as a component. Then $C_{s'} \cdot E$ contains $\Sigma mP_i + \Sigma_1{}^{(r-s)/2} mQ_i$. Since $\deg C_{s'} \cdot E = ss'm = s(s+1)m/2$, we have $C_{s'} \cdot E = \Sigma mP_i + \Sigma_1{}^{(r-s)/2} mQ_i$. Since $s \geqq 5$, $s' \geqq 3$, hence $C_{s'}$ is of positive genus. Since the P_i are independent generic points of $C_{s'}$ over $\pi(C_{s'}, Q_1, \cdots, Q_{(r-s)/2})$, we have a contradiction by the following obvious

LEMMA 5. *If C is a plane curve of positive genus and if $R_1, \cdots, R_n$ are points of C such that some of the R_i are independent generic points of C over a field of definition of C and the other R_i's, then for any natural numbers $c_1, \cdots, c_n$, there exists no curve whose intersection with C is equal to $\Sigma c_i R_i$.*

Therefore E must contain $C_{s'}$ as a component. Similarly, E must contain $C'_{s'}$ as a component. Then, specializing $E - C_{s'} - C'_{s'}$ over the specialization we considered above, we see the existence of a curve E^* of degree $s(m-1)-1$ which goes through the P^*_i with multiplicity at least $m-2$ and the Q^*_j with multiplicity at least $m-1$. Hence, if $m=1$, we have a contradiction. We shall use the induction on m. Assume that E^* does not contain C_s as a component. Then $C_s \cdot E^*$ contains $\Sigma(m-2)P^*_i + \Sigma(m-1)Q^*_j$. By the equality of the degrees, we have $C_s \cdot E^* = \Sigma(m-2)P^*_i + \Sigma(m-1)Q^*_j$. Since $C_s(C_{s'} + C'_{s'}) = \Sigma 2P^*_i + \Sigma Q^*_j$, we have $C_s \cdot ((m-1)(C_{s'} + C'_{s'}) - E^*) = \Sigma mP^*_i$, which gives a contradiction by Lemma 5. Thus E^* must contain C_s as a component and we have a contradiction by induction on m.

(ii) The case where r is even. Set $s' = (s+2)/2$ and let C_s, $C_{s'}$, $C'_{s'}$ be independent generic curves of degree s, s', s' respectively. Let $P_1, \cdots, P_{2s}$

be $2s$ points among $C_{s'} \cdot C'_{s'}$. Then we take independent generic points $P^*_1, \cdots, P^*_{2s}$ of C_s over $\pi(C_s)$. Then we prove the assertion by the same way as in (i) and we omit the detail (cf. [5]).

Remark. In order to satisfy the requirement in § 1 for r, r must be greater than 9.

Proof. If $r = 1$ or 2, then there is a line going through P_i; if $r = 3$, the sum of 3 lines going through two of the P_i gives a counter-example to the requirement; if $r = 4$ or 5, then there is a conic going through the P_i; if $r = 6$, the sum of 6 conics going through 5 of the P_i gives a counter-example; if $r = 7$, sum of 7 cubics each of which has a double point at one of the P_i and goes through all the P_i gives a counter-example; if $r = 8$, the sum of 8 curves of degree 6 each of which has a triple point at one of the P_i and has double points at all the other P_i gives a counter-example; if $r = 9$, then there is a cubic going through all the P_i.

The writer has the following conjecture:

CONJECTURE. *For the requirement in* § 1 *for r, it will be enough for r to be greater than* 9.

HARVARD UNIVERSITY AND KYOTO UNIVERSITY.

REFERENCES.

[1] D. Hilbert, "Mathematische Probleme," *Archiv f. Math. Phys.*, ser. 3, vol. 1 (1901), pp. 44-63; pp. 213-237.

[2] O. Zariski, "Interprétations algébrico-géométriques du quatorzième problème de Hilbert," *Bull. Sci. Math.*, vol. 78 (1954), pp. 155-168.

[3] M. Nagata, "A treatise on the 14-th problem of Hilbert," *Memoirs Coll. Sci. Univ. Kyoto, ser. A Math.*, vol. 30 (1956-57), pp. 57-70; Addition and corrections to it, pp. 197-200.

[4] D. Rees, "On a problem of Zariski," *Illinois Journal of Mathematics*, vol. 2 (1958), pp. 145-149.

[5] M. Nagata, "On the 14-th problem of Hilbert," to appear in *Proceedings of the International Congress of Mathematicians*, Edinburgh, 1958.

A NOTE ON OBSTRUCTIONS AND CHARACTERISTIC CLASSES.*

By Michel A. Kervaire.

The present paper is a generalization of [7]. Relations will be established between the obstructions associated with cross-sections in a stable $\boldsymbol{U}(n)$, $\boldsymbol{SO}(n)$ or $\boldsymbol{Sp}(n)$-bundle over a *complex* K and the characteristic classes of such bundles.

In the $\boldsymbol{U}(n)$-case, we obtain as a corollary a theorem of F. Peterson [10] stating that a $\boldsymbol{U}(n)$-bundle over a torsion free complex K of dimension $\leqq 2n$ is trivial if and only if the Chern classes of the bundle vanish.

A similar statement in the $\boldsymbol{SO}(n)$ or $\boldsymbol{Sp}(n)$ case, involving the Pontryagin, resp. symplectic Pontryagin classes, would be wrong. In case of an $\boldsymbol{SO}(n)$ [resp. $\boldsymbol{Sp}(n)$] bundle there are obstructions in $H^{8s+1}(K;\boldsymbol{Z}_2)$ and $H^{8s+2}(K;\boldsymbol{Z}_2)$ [resp. $H^{8s+5}(K;\boldsymbol{Z}_2)$ and $H^{8s+6}(K;\boldsymbol{Z}_2)$] which are not expressible in terms of characteristic classes of the bundle (see Lemma 4.3 for a precise statement). The information about these obstructions is still very poor.

In [10], F. Peterson deduces his theorem from a computation of the Postnikov decomposition of $B_{\boldsymbol{U}(n)}$. We proceed the other way around and obtain the Postnikov decomposition of $B_{\boldsymbol{U}(n)}$, $B_{\boldsymbol{SO}(n)}$ and $B_{\boldsymbol{Sp}(n)}$ in the stable range from the main lemma (Lemma 1.1).

I am indebted to J. Milnor, B. Eckmann and A. Borel for their suggestions during the preparation of this paper.

1. Let $\boldsymbol{G}$ be one of the groups $\boldsymbol{U}(n)$, $\boldsymbol{SO}(n)$ or $\boldsymbol{Sp}(n)$. Let ξ be a stable principal $\boldsymbol{G}$-bundle over a CW-complex K (stability means that the homotopy groups $\pi_{q-1}(\boldsymbol{G})$ are stable for $q \leqq \dim K$). Assume that ξ admits a cross-section f over the $(q-1)$-skeleton $K^{(q-1)}$ of K. Take q to be even $=2r$ if $\boldsymbol{G}=\boldsymbol{U}(n)$ and q divisible by 4, $q=4k$, if $\boldsymbol{G}=\boldsymbol{SO}(n)$ or $\boldsymbol{Sp}(n)$. Then, by [4], $\pi_{q-1}(\boldsymbol{G}) \approx \boldsymbol{Z}$ in all cases. The obstruction class $\mathfrak{o}(\xi,f) \in H^q(K;\pi_{q-1}(\boldsymbol{G}))$ to extending f over the q-skeleton can be regarded up to sign as an integer class. Denote by $c_r(\xi)$, $p_k(\xi)$, $e_k(\xi)$ the Chern class, the Pontryagin or the symplectic Pontryagin class[1] of ξ in dimension q according as $\boldsymbol{G}=\boldsymbol{U}(n)$, $\boldsymbol{SO}(n)$ or $\boldsymbol{Sp}(n)$ respectively.

* Received October 5, 1958.

[1] See [3], 9.6, for the definition.

LEMMA 1.1. *The characteristic classes $c_r(\xi)$, $p_k(\xi)$, $e_k(\xi)$ are given by the formulae*

$$\text{(i)} \qquad c_r(\xi) = (r-1)!\,\mathfrak{o}(\xi, f) \qquad \text{if } \boldsymbol{G} = \boldsymbol{U}(n),$$

$$\text{(ii)} \qquad p_k(\xi) = (2k-1)!\,a_k\mathfrak{o}(\xi, f) \qquad \text{if } \boldsymbol{G} = \boldsymbol{SO}(n),$$

$$\text{(iii)} \qquad e_k(\xi) = (2k-1)!\,b_k\mathfrak{o}(\xi, f) \qquad \text{if } \boldsymbol{G} = \boldsymbol{Sp}(n),$$

where, as in [6], $a_k \cdot b_k = 2$ and a_k is equal to 1 for k even and to 2 for k odd.

Proof. Let $\boldsymbol{G} = \boldsymbol{U}(n)$. Denote by ξ' the associated bundle with fibre $W_{n,n-r+1} = \boldsymbol{U}(n)/\boldsymbol{U}(r-1)$. Let $q\colon \boldsymbol{U}(n) \to \boldsymbol{U}(n)/\boldsymbol{U}(r-1)$ be the natural projection and q' the induced map of the total space of ξ into the total space of ξ'. The map $f' = q' \circ f$ is a cross-section of ξ' restricted to the $(q-1)$-skeleton. Denote by $q_*\colon \pi_{2r-1}(\boldsymbol{U}(n)) \to \pi_{2r-1}(W_{n,n-r+1})$ and

$$q_{**}\colon H^{2r}(K; \pi_{2r-1}(\boldsymbol{U}(n))) \to H^{2r}(K; \pi_{2r-1}(W_{n,n-r+1}))$$

the homomorphisms induced by q. Clearly, $q_{**}\mathfrak{o}(\xi, f) = \mathfrak{o}(\xi', f') =$ the obstruction to extending f' over the $2r$-skeleton. In other words $q_{**}\mathfrak{o}(\xi, f) = c_r(\xi)$. Identifying $\pi_{2r-1}(\boldsymbol{U}(n))$ and $\pi_{2r-1}(W_{n,n-r+1})$ with $\boldsymbol{Z}$ (disregarding signs), we have $q_{**}u = (r-1)!\,u$ for any $u \in H^*(K; \boldsymbol{Z})$ because q_* maps a generator of $\pi_{2r-1}(\boldsymbol{U}(n))$ onto $(r-1)!$ times a generator of $\pi_{2r-1}(W_{n,n-r+1})$ according to [5]. Thus $c_r(\xi) = q_{**}\mathfrak{o}(\xi, f) = \pm(r-1)!\,\mathfrak{o}(\xi, f)$.

The proofs of (ii) and (iii) are entirely similar and are left to the reader (compare also [9]).

2. As a corollary we obtain the

THEOREM 2.1 (F. Peterson). *Let ξ be a $\boldsymbol{U}(n)$-bundle over a complex K with $\dim K \leq 2n$ and assume that $H^{2r}(K; \boldsymbol{Z})$ has no torsion except possibly prime to $(r-1)!$ for $r = 1, 2, \cdots$. Then ξ is trivial if and only if the Chern classes $c_1, \cdots, c_n$ vanish.*

Proof. Half of the statement is trivial. We prove that ξ is the product bundle provided $c_1(\xi) = 0$, $c_2(\xi) = 0, \cdots, c_n(\xi) = 0$ by stepwise extension of a cross-section in the associated principal bundle ξ_P.

If f is a cross-section in ξ_P restricted to $K^{(q-1)}$ and q is odd, there is no obstruction to extending f to $K^{(q)}$ since $\pi_{2i}(\boldsymbol{U}(n)) = 0$ for $i < n$ by [4]. Let q be even: $q = 2r$. Then by Lemma 1.1 the obstruction class $\mathfrak{o}(\xi, f)$ satisfies the identity $c_r = \pm(r-1)!\,\mathfrak{o}(\xi, f)$. Under the assumptions of the theorem this implies $\mathfrak{o}(\xi, f) = 0$. It follows (see [11], 34.2) that $f \mid K^{(q-2)}$ is extendable over $K^{(q)}$. This proves the theorem by induction on q.

Some information on the obstructions arising in the $\boldsymbol{SO}(n)$ and $\boldsymbol{Sp}(n)$ cases is given in Lemmas 4.1 and 4.2 below. We need a preliminary lemma.

3. Let $\boldsymbol{G}$ be any Lie group and $\boldsymbol{H}$ a closed subgroup of $\boldsymbol{G}$ such that the sequence

$$(3.1) \qquad 0 \to \pi_q(\boldsymbol{G}/\boldsymbol{H}) \xrightarrow{\partial} \pi_{q-1}(\boldsymbol{H}) \xrightarrow{i_*} \pi_{q-1}(\boldsymbol{G}) \to 0$$

is exact for some q (here i_* is induced by the inclusion $i\colon \boldsymbol{H} \to \boldsymbol{G}$). Assume that the $\boldsymbol{G}$-bundle ξ over the complex K admits a cross-section f over the $(q-1)$-skeleton. Let $\mathfrak{o}(\xi, f) \in H^q(K; \pi_{q-1}(\boldsymbol{G}))$ be the obstruction class to extending f over $K^{(q)}$. We want to compute $\delta^*\mathfrak{o}(\xi, f)$, where δ^* is the boundary homomorphism $\delta^*\colon H^q(K; \pi_{q-1}(\boldsymbol{G})) \to H^{q+1}(K; \pi_q(\boldsymbol{G}/\boldsymbol{H}))$ of the cohomology exact sequence associated with the coefficient sequence (3.1). (Compare Steenrod [11], 38.5.)

Let ξ' be the associated bundle with fibre $\boldsymbol{G}/\boldsymbol{H}$. The cross-section f induces a cross-section f' of ξ' restricted to the $(q-1)$-skeleton.

LEMMA 3.2. *Under the above exactness assumption of* (3.1), *the cross-section f' is always extendable to a cross-section F' of ξ' restricted to $K^{(q)}$. Let $\mathfrak{o}(\xi', F') \in H^{q+1}(K; \pi_q(\boldsymbol{G}/\boldsymbol{H}))$ be the obstruction class to extending F' over $K^{(q+1)}$. Then $\delta^*\mathfrak{o}(\xi, f) = \mathfrak{o}(\xi', F')$.*

Proof. Let $p\colon \pi_{q-1}(\boldsymbol{G}) \to \pi_{q-1}(\boldsymbol{G}/\boldsymbol{H})$ be induced by the projection $\boldsymbol{G} \to \boldsymbol{G}/\boldsymbol{H}$, and $p_*\colon Z^q(K; \pi_{q-1}(\boldsymbol{G})) \to Z^q(K; \pi_{q-1}(\boldsymbol{G}/\boldsymbol{H}))$ be the homomorphism induced by the coefficient homomorphism p. Let $z \in \mathfrak{o}(\xi, f)$ be the obstruction *cocycle* to extending f over $K^{(q)}$ and z' be the obstruction cocycle to extending f' over $K^{(q)}$. We have $p_* z = z'$ and since p is zero, it follows $z' = 0$. In other words, f' can be extended to a cross-section F' of ξ' restricted to $K^{(q)}$. The map $F'\colon K^{(q)} \to E'$, where E' is the total space of ξ' induces over $K^{(q)}$ an $\boldsymbol{H}$-bundle η (E' is the quotient of the total space E of ξ by the action of $\boldsymbol{H}$ as a subgroup of $\boldsymbol{G}$). $f_\eta(x) = (x, f(x))$ for $x \in K^{(q-1)}$ defines a cross-section of η restricted to $K^{(q-1)}$ (compare Steenrod [11], 10.2). Let $u_\eta \in Z^q(K^{(q)}; \pi_{q-1}(\boldsymbol{H}))$ be the obstruction cocycle to extending f_η over $K^{(q)}$ and let $u \in C^q(K; \pi_{q-1}(\boldsymbol{H}))$ be defined by $u[\tau] = u_\eta[\tau]$ for every q-cell $\tau \in K^{(q)} \subset K$. Clearly, $i_{**} u = z$, where $i_{**}\colon C^q(K; \pi_{q-1}(\boldsymbol{H})) \to C^q(K; \pi_{q-1}(\boldsymbol{G}))$ is induced by $i_*\colon \pi_{q-1}(\boldsymbol{H}) \to \pi_{q-1}(\boldsymbol{G})$. The assertion of the lemma can be stated as

$$(3.3) \qquad \delta u = \partial_* z',$$

where $\partial_*\colon Z^{q+1}(K; \pi_q(\boldsymbol{G}/\boldsymbol{H})) \to Z^{q+1}(K; \pi_{q-1}(\boldsymbol{H}))$ is induced by $\partial\colon \pi_q(\boldsymbol{G}/\boldsymbol{H})$

$\to \pi_{q-1}(\boldsymbol{H})$, and z' is the obstruction to extending F' over $K^{(q+1)}$. (Compare Steenrod [11], 38.5 formula (8).)

Let $\Phi: B^{q+1} \to K$ be the attaching map of a $(q+1)$-cell σ of K, and denote by ϕ the restriction of Φ to the boundary S^q of B^{q+1}. Then $F' \circ \phi: S^q \to E'$ induces over S^q an $\boldsymbol{H}$-bundle whose characteristic map $\chi = \Delta\alpha$ is the image of the element $\alpha \in \pi_q(E')$ represented by $F' \circ \phi$ under the boundary operator $\Delta: \pi_q(E') \to \pi_{q-1}(H)$ of the homotopy sequence of $H \to E \xrightarrow{\pi} E'$. Since $F' \circ \phi(S^q) \subset \rho^{-1}(\Phi B)$, where ρ is the projection $\rho: E' \to K$ of the bundle ξ', $F' \circ \phi$ as a map in $\rho^{-1}(\Phi B)$ represents an element of $\pi_q(G/H)$ which is equal to $z'[\sigma]$. Thus $j'_*(z'[\sigma]) = \alpha$, where $j': \boldsymbol{G}/\boldsymbol{H} \to E'$ is the inclusion of the fibre. On the other hand χ is equal to $u[\phi S^q]$. Consider the commutative diagram

$$\begin{array}{ccc} \pi_q(\boldsymbol{G}/\boldsymbol{H}) & \xrightarrow{\partial} & \pi_{q-1}(\boldsymbol{H}) \\ \Big\downarrow j'_* & & \Big\| \\ \pi_q(E') & \xrightarrow{\Delta} & \pi_{q-1}(\boldsymbol{H}) \end{array}$$

induced by the bundle map

$$\begin{array}{ccc} \boldsymbol{G} & \xrightarrow{j} & E \\ p\Big\downarrow & & \Big\downarrow\pi \\ \boldsymbol{G}/\boldsymbol{H} & \xrightarrow{j'} & E'. \end{array}$$

We have

$$\delta u[\sigma] = u[\phi S^q] = \Delta\alpha = \Delta j'_*(z'[\sigma]) = \partial_*(z'[\sigma]) = (\partial_* z')[\sigma].$$

Since this is true for any $(q+1)$-cell σ, the proof of (3.3) is complete.

4. We apply this to the cases $\boldsymbol{G} = \boldsymbol{SO}(2n)$ and $\boldsymbol{G} = \boldsymbol{Sp}(n)$, $\boldsymbol{H} = \boldsymbol{U}(n)$.

LEMMA 4.1. *Let the stable principal $\boldsymbol{SO}(2n)$-bundle ξ admit a cross-section f over the $(8s+1)$-skeleton $K^{(8s+1)}$ of the base complex K. Let $\mathfrak{o}(\xi, f) \in H^{8s+2}(K; \boldsymbol{Z}_2)$ be the obstruction class* (compare Bott [4]). *The induced cross-section f' of the associated bundle ξ' with fibre $\boldsymbol{SO}(2n)/\boldsymbol{U}(n)$ restricted to $K^{(8s+1)}$ is extendable over $K^{(8s+2)}$ to a cross-section F'. One has $\beta\mathfrak{o}(\xi, f) = \pm\, \mathfrak{o}(\xi', F')$, where β is the Bockstein operation and $\mathfrak{o}(\xi', F')$ is the obstruction class to extending F' over $K^{(8s+3)}$.*

Proof. Take $\boldsymbol{G} = \boldsymbol{SO}(2n)$ and $\boldsymbol{H} = \boldsymbol{U}(n)$ in Lemma 3.2. The sequence

$$0 \to \pi_{8s+2}(\boldsymbol{SO}(2n)/\boldsymbol{U}(n)) \to \pi_{8s+1}(\boldsymbol{U}(n)) \to \pi_{8s+1}(\boldsymbol{SO}(2n)) \to 0$$

is exact and reads $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}_2 \to 0$. (Compare Bott [4].) The associated coboundary homomorphism δ^* is β by definition. Similarly,

LEMMA 4.2. *Let the stable principal $\mathbf{Sp}(n)$-bundle ξ admit a cross-section f over the $(8s+5)$-skeleton of the base complex K. Denote by $\mathfrak{o}(\xi, f) \in H^{8s+6}(K; \mathbf{Z}_2)$ the obstruction class. f induces a cross-section f' of the associated bundle ξ' with fibre $\mathbf{Sp}(n)/\mathbf{U}(n)$ restricted to $K^{(8s+5)}$. Then f' is extendable over the $(8s+6)$-skeleton. Let F' be an extension and $\mathfrak{o}(\xi', F') \in H^{8s+7}(K; \mathbf{Z})$ the obstruction class (up to sign). We have $\beta\mathfrak{o}(\xi, f) = \pm\, \mathfrak{o}(\xi', F')$.*

Proof. The sequence

$$0 \to \pi_{8s+6}(\mathbf{Sp}(n)/\mathbf{U}(n)) \to \pi_{8s+5}(\mathbf{U}(n)) \to \pi_{8s+5}(\mathbf{Sp}(n)) \to 0$$

is exact and reads $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}_2 \to 0$. (Compare Bott [4].)

Next we show that the Stiefel-Whitney class w_q of an $\mathbf{SO}(n)$-bundle ξ is in general independent of the obstruction to extending over $K^{(q)}$ a cross-section of ξ restricted to $K^{(q-1)}$. In fact:

LEMMA 4.3. *If there exists a cross-section of the $\mathbf{SO}(n)$-bundle ξ restricted to the $(q-1)$-skeleton of the base complex K, $q > 0$ and $q \neq 2$, 4, 8, then the Stiefel-Whitney class w_q of ξ is zero.*

Proof. Let $\mathfrak{o}(\xi, f)$ be the cohomology class of the obstruction to extending the given cross-section f over the q-skeleton. Let $p\colon \mathbf{SO}(n) \to V_{n,n-q+1} = \mathbf{SO}(n)/\mathbf{SO}(q-1)$ be the natural projection, and

$$p_*\colon \pi_{q-1}(\mathbf{SO}(n)) \to \pi_{q-1}(V_{n,n-q+1}),$$
$$p_{**}\colon H^q(K; \pi_{q-1}(\mathbf{SO}(n))) \to H^q(K; \pi_{q-1}(V_{n,n-q+1}))$$

the induced homomorphisms. Clearly, $p_{**}\mathfrak{o}(\xi, f) = w_q$. The lemma follows from the fact that p_* is zero provided $q \neq 2, 4, 8$. This is trivial for $q \equiv 3$, $5, 6, 7$ modulo 8 ($\pi_{q-1}(\mathbf{SO}(n))$ is zero in these cases by [4]). It is also trivial for $q \equiv 1 \bmod 8$ since $\pi_0(\mathbf{SO}(n)) = 0$ and $\pi_{8s}(\mathbf{SO}(n)) = \mathbf{Z}_2$, $\pi_{8s}(V_{n,n-8s}) \approx \mathbf{Z}$ for $s > 0$. For $q \equiv 2 \bmod 8$, $p_* = 0$ follows easily from considering the homotopy exact sequence of $\mathbf{SO}(n)/\mathbf{SO}(q-1)$. For $q \equiv 4 \bmod 8$, $p_* = 0$ was stated and proved in [6], Lemma 3. The case $q \equiv 0 \bmod 8$ will be treated in a forth coming paper [8].[2]

Using the Lemma 1.1 above, we obtain the k-invariants of the classifying spaces $B_{\mathbf{U}(n)}$, $B_{\mathbf{SO}(n)}$, $B_{\mathbf{Sp}(n)}$ in the *stable range*. (For the k-invariants of

[2] (Added in proof) $p_* = 0$ also follows from comparison with $p'_*\colon \pi_{q-1}(\mathbf{SO}(q)) \to \pi_{q-1}(S^{q-1})$ as in the proof of Lemma 6.4 below.

$B_{U(n)}$, compare F. Peterson [10]). We need a few probably well known lemmas about k-invariants which we derive in the next section.

5. Let X be a simply connected space and $X_q \supset X$ such that

(i) (X_q, X) is a relative CW-complex (compare G. W. Whitehead [12]),

(ii) $\pi_i(X_q) = 0$ for $q < i$,

(iii) $\pi_i(X) \approx \pi_i(X_q)$ for $i \leqq q$ under inclusion.

Then, $\pi_i(X_q, X) = 0$ for $i \leqq q+1$ and since $\pi_1(X) = 0$ by assumption, it follows from the relative Hurewicz theorem that $H_i(X_q, X) = 0$ for $i \leqq q+1$, and $\pi_{q+1}(X) \approx \pi_{q+2}(X_q, X) \approx H_{q+2}(X_q, X)$. It follows that $H^{q+2}(X_q, X; \pi_{q+1}) = \mathrm{Hom}(H_{q+2}(X_q, X), \pi_{q+1})$ contains a fundamental class u (π_{q+1} denotes $\pi_{q+1}(X)$ for brevity).

LEMMA 5.1. *$a^*u = k^{q+2} \in H^{q+2}(X_q; \pi_{q+1})$ is the $(q+2)$-dimensional k-invariant of X, where $a^*\colon H^*(X_q, X; \pi_{q+1}) \to H^*(X_q; \pi_{q+1})$ is induced by the inclusion $a\colon (X_q, 0) \to (X_q, X)$.*

In fact the lemma is a special case of the following definition of the characteristic class.

Let $p\colon E \to B$ be a fibering with q-connected fibre F, and let $i\colon F \to E$ be the inclusion of the fibre. Assume that E (and thus also B) is simply connected. By the homotopy exact sequence, $p_*\colon \pi_i(E) \to \pi_i(B)$ is an isomorphism for $i \leqq q$, and $p_*\colon \pi_{q+1}(E) \to \pi_{q+1}(B)$ is surjective. Therefore, $\pi_i(B', E) = 0$ for $i \leqq q+1$, where B' is the mapping cylinder of p (B and B' have the same homotopy type). Since $\pi_1(E) = 0$, it follows $H_i(B', E) = 0$ for $i \leqq q+1$, and $\pi_{q+2}(B', E) \approx H_{q+2}(B', E)$. Thus $H^{q+2}(B', E; \pi_{q+2}(B', E)) = \mathrm{Hom}(H_{q+2}(B', E), \pi_{q-2}(B', E))$ contains a fundamental class u.

Define a homomorphism $\phi\colon \pi_i(F) \to \pi_{i+1}(B', E)$ for every i as follows: If $f\colon S^i \to F$ represents a class $\alpha \in \pi_i(F)$, the formula

$$f'(x, t) = (f(x), t),$$

$0 \leqq t \leqq 1$ defines a mapping of the cone over S^i into B'. The boundary of this cone is mapped into $F \subset E$. Let $\phi\alpha$ be the class of f' in $\pi_{i+1}(B', E)$.

LEMMA 5.1′. *ϕ is an isomorphism, and $\phi_* c = a^*u$, where ϕ_* is induced by the coefficient homomorphism $\phi\colon \pi_{q+1}(F) \to \pi_{q+2}(B', E)$; c is the characteristic class and a^* is induced by the inclusion $(B', 0) \subset (B', E)$.*

Proof. Consider the diagram

$$\begin{array}{ccccccccc}
\pi_{i+1}(E) & \longrightarrow & \pi_{i+1}(E,F) & \xrightarrow{\partial} & \pi_i(F) & \xrightarrow{i_*} & \pi_i(E) & \longrightarrow & \pi_i(E,F) \\
\downarrow \text{id.} & & \downarrow p_* & & \downarrow \phi & & \downarrow \text{id.} & & \downarrow p_* \\
\pi_{i+1}(E) & \xrightarrow{p_*} & \pi_{i+1}(B) & \xrightarrow{a_*} & \pi_{i+1}(B',E) & \xrightarrow{\partial'} & \pi_i(E) & \xrightarrow{p_*} & \pi_i(B).
\end{array}$$

It is easily seen from the definition of ϕ that commutativity holds in each square. Since p_* is an isomorphism, ϕ is an isomorphism by the 5-Lemma.

Let $\psi\colon H_i(F) \to H_{i+1}(B',E)$ be defined similarly to ϕ. The cycle z being a representative of a class $\zeta \in H_i(F)$, $\psi\zeta$ is the class in $H_{i+1}(B',E)$ of the cone over z in B', regarded as a cycle modulo E. Clearly, the following diagram is commutative:

$$\begin{array}{ccccccccc}
H_{i+1}(E) & \longrightarrow & H_{i+1}(E,F) & \xrightarrow{\partial} & H_i(F) & \xrightarrow{i_*} & H_i(E) & \longrightarrow & H_i(E,F) \\
\downarrow \text{id.} & & \downarrow p_* & & \downarrow \psi & & \downarrow \text{id.} & & \downarrow p_* \\
H_{i+1}(E) & \longrightarrow & H_{i+1}(B) & \xrightarrow{a_*} & H_{i+1}(B',E) & \xrightarrow{\partial'} & H_i(E) & \longrightarrow & H_i(B).
\end{array}$$

It follows by a standard argument that the dual diagram with coefficient group $\pi_j(F) = \pi_{j+1}(B',E)$, identified by $\phi\colon \pi_j(F) \to \pi_{j+1}(B',E)$, is also commutative. In particular,

$$\begin{array}{ccc}
H^{q+2}(E,F;\pi_{q+1}) & \xleftarrow{\delta} & H^{q+1}(F;\pi_{q+1}) \\
\uparrow p^* & & \uparrow \psi^* \\
H^{q+2}(B;\pi_{q+1}) & \xleftarrow{a^*} & H^{q+2}(B',E;\pi_{q+1})
\end{array}$$

is commutative (π_{q+1} denotes $\pi_{q+1}(F)$ identified with $\pi_{q+2}(B',E)$ by ϕ). Since c is characterized by $p^*c = \delta v$, where v is the fundamental class in $H^{q+1}(F;\pi_{q+1})$, it remains only to prove that $\psi^*u = v$. This is obvious, and the proof of Lemma 5.1′ is complete.

Consider the cohomology exact sequence

$$\cdots \to H^{q+1}(X;\pi_{q+1}) \xrightarrow{\delta} H^{q+2}(X_q,X;\pi_{q+1}) \xrightarrow{a^*} H^{q+2}(X_q;\pi_{q+1}) \to \cdots$$

Clearly, δ annihilates every decomposable element of $H^{q+1}(X;\pi_{q+1})$.

In fact, if $c \in H^{q+1}(X;\pi_{q+1})$ is any class, δc as a homomorphism of π_{q+1} into π_{q+1} is given by

$$\delta c[\alpha] = \alpha^* c, \text{ for every } \alpha \in \pi_{q+1}, \tag{5.2}$$

where $\alpha^*\colon H^{q+1}(X;\pi_{q+1}) \to H^{q+1}(S^{q+1};\pi_{q+1})$ is induced by any map $S^{q+1} \to X$ representing α, and $H^{q+1}(S^{q+1};\pi_{q+1})$ is identified with π_{q+1}.

6. As an application of Lemma 1.1 and the preceding remarks, we obtain:

THEOREM 6.1. *Let* $X = B_{U(n)}$ *and* $\pi_{q+1} = \pi_{q+1}(B_{U(n)}) \approx \pi_q(U(n))$. *Then, for* $i < n$, *we have* $\boldsymbol{k}^{2i+2} = 0$, *and* X_{2i+1} *may be taken equal to* X_{2i}. $H^{2i+3}(X_{2i+1}; \pi_{2i+2}) = H^{2i+3}(X_{2i+1}; \boldsymbol{Z})$ *is a finite cyclic group of order* $i!$ *generated by the k-invariant* $\boldsymbol{k}^{2i+3}$.

THEOREM 6.2. *Let* $X = B_{SO(n)}$ *and* $\pi_{q+1} = \pi_{q+1}(B_{SO(n)}) \approx \pi_q(\boldsymbol{SO}(n))$. *Then, in the stable range,* $\boldsymbol{k}^{4j} = 0$, $\boldsymbol{k}^{8i-2} = 0$, $\boldsymbol{k}^{8i-1} = 0$. *One can take* $X_{4j-1} = X_{4j-2}$, $X_{8i-2} = X_{8i-3} = X_{8i-4}$. *The k-invariants* $\boldsymbol{k}^{4j+1}$, $\boldsymbol{k}^{8i+2}$, $\boldsymbol{k}^{8i+3}$ *are different from zero. Specifically, we have exact sequences*

$$(6.2') \qquad 0 \to \boldsymbol{Z}_{(2j-1)!a_j} \xrightarrow{\bar{a}^*} H^{4j+1}(X_{4j-1}; \pi_{4j}) \to H^{4j+1}(X; \pi_{4j}) \to 0$$

which split for $j \geqq 3$. *The k-invariant* $\boldsymbol{k}^{4j+1}$ *is the image under* $\bar{a}^*$ *of a generator of* $\boldsymbol{Z}_{(2j-1)!a_j}$. *For* $j = 1$ *or* 2, $\boldsymbol{k}^{4j+1}$ *can be halved and* $\frac{1}{2}\boldsymbol{k}^{4j+1}$ *can be chosen so as to project onto* $W^{4j+1} \in H^{4j+1}(X; \pi_{4j})$. *Similarly, the sequences*

$$(6.2'') \qquad \begin{gathered} 0 \to \boldsymbol{Z}_2 \xrightarrow{a^*} H^{8i+2}(X_{8i}; \pi_{8i+1}) \to H^{8i+2}(X; \pi_{8i+1}) \to 0, \\ 0 \to \boldsymbol{Z}_2 \xrightarrow{a^*} H^{8i+3}(X_{8i+1}; \pi_{8i+2}) \to H^{8i+3}(X; \pi_{8i+2}) \to 0, \end{gathered}$$

are exact and split. $\boldsymbol{k}^{8i+2}$, *resp.* $\boldsymbol{k}^{8i+3}$ *are the images under* a^* *of the generator of* $\boldsymbol{Z}_2$. ($\pi_{4j} \approx \boldsymbol{Z}$, $\pi_{8i+1} \approx \pi_{8i+2} \approx \boldsymbol{Z}_2$, by [4].)

THEOREM 6.3. *Let* $X = B_{Sp(n)}$ *and* $\pi_{q+1} = \pi_{q+1}(B_{Sp(n)}) \approx \pi_q(\boldsymbol{Sp}(n))$. *Then, in the stable range,* $\boldsymbol{k}^{4j} = 0$, $\boldsymbol{k}^{8i+2} = 0$, $\boldsymbol{k}^{8i+3} = 0$. *One can take* $X_{4j-1} = X_{4j-2}$, $X_{8i+2} = X_{8i+1} = X_{8i}$. *The other k-invariants are non-zero. Precisely,*

$$H^{4j+1}(X_{4j-1}; \boldsymbol{Z}) \approx \boldsymbol{Z}_{(2j-1)!b_j} \text{ generated by } \boldsymbol{k}^{4j+1},$$

$$H^{8i-2}(X_{8i-4}; \boldsymbol{Z}_2) \approx \boldsymbol{Z}_2 \text{ generated by } \boldsymbol{k}^{8i-2},$$

$$H^{8i-1}(X_{8i-3}; \boldsymbol{Z}_2) \approx \boldsymbol{Z}_2 \text{ generated by } \boldsymbol{k}^{8i-1}.$$

Proof of Theorem 6.1. The first assertion is trivial since $\pi_{2i+1}(B_{U(n)}) = 0$ for $i < n$. Consider the cohomology exact sequence

$$H^{2i+2}(X) \xrightarrow{\delta} H^{2i+3}(X_{2i+1}, X) \xrightarrow{a^*} H^{2i+3}(X_{2i+1}) \to H^{2i+3}(X)$$

with coefficients in $\pi_{2i+2}(X) \approx \boldsymbol{Z}$. Since $H^*(X) \approx \boldsymbol{Z}[c_1, \cdots, c_n]$, $\deg c_j = 2j$ (see [2], Theorem 21.3), we have $H^{2i+3}(X) = 0$ and $H^{2i+2}(X)$ is the direct

sum of $\pi(i+1)$ copies of $\boldsymbol{Z}$, where $\pi(i+1)$ is the number of partitions of $i+1$. By (5.2) and Lemma (1.1), δ is zero on the decomposable elements and $\delta c_{i+1} = \pm\, i!\cdot u$, where u is the fundamental class in $H^{2i+3}(X_{2i+1}, X) \approx \boldsymbol{Z}$. It follows that $H^{2i+3}(X_{2i+1})$ is cyclic of order $i!$, generated by $a^*u = \boldsymbol{k}^{2i+3}$.

Proof of Theorem 6.2. The first assertions are trivial since $\pi_{4j-2}(\boldsymbol{SO}(n))$, $\pi_{8i-4}(\boldsymbol{SO}(n))$ and $\pi_{8i-3}(\boldsymbol{SO}(n))$ are zero in the stable range (see [4]). Consider the cohomology exact sequence.

$$H^{4j}(X) \xrightarrow{\delta} H^{4j+1}(X_{4j-1}, X) \xrightarrow{a^*} H^{4j+1}(X_{4j-1}) \to H^{4j+1}(X) \xrightarrow{\delta'}$$

with coefficients in $\pi_{4j}(B_{SO(n)}) \approx \boldsymbol{Z}$. Since $H^*(B_{SO};\boldsymbol{R}) = \boldsymbol{R}[p_1,\cdots,p_r,\cdots]$, $H^*(B_{SO(n)};\boldsymbol{Z}_2) = \boldsymbol{Z}_2[w_2,\cdots,w_n]$, and $B_{SO(n)}$ has no other torsion than 2-torsion (see [3], Appendix II), every class $c \in H^*(B_{SO(n)})$ with $\deg c < n$ can be written in the form $c = P(p_1,\cdots,p_r) + \beta Q(w_2,\cdots,w_s)$, where β is the Bockstein homomorphism and P, Q are polynomials. Hence, $\delta\colon H^{4j}(X) \to H^{4j+1}(X_{4j-1}, X)$ kills every element except possibly p_j. It follows from (5.2) and Lemma (1.1) that $\delta p_j = \pm(2j-1)!\,a_j\cdot u$, where $u \in H^{4j+1}(X_{4j-1}, X)$ is the fundamental class. If $c \in H^{4j+1}(X)$, it has the form $\beta c'$, with $c' \in H^{4j}(X;\boldsymbol{Z}_2)$. Thus $\delta' c = 0$, except possibly if $c = \beta w_{4j} = W_{4j+1}$, and then $\delta' W_{4j+1} = \beta\delta w_{4j}$. Since by (5.2) δw_{4j} is the $4j$-dimensional Stiefel-Whitney class of the $\boldsymbol{SO}(n)$-bundle induced over S^{4j} by a map $S^{4j} \to B_{SO(n)}$ representing a generator of $\pi_{4j}(B_{SO(n)}) \approx \boldsymbol{Z}$, we obtain information about δw_{4j} from the following lemma:

LEMMA 6.4. *Let ξ be the stable $\boldsymbol{SO}(n)$-bundle induced over S^{4j} by a map representing a generator of $\pi_{4j}(B_{SO(n)}) \approx \boldsymbol{Z}$. The Stiefel-Whitney class $w_{4j}(\xi) \in H^{4j}(S^{4j};Z_2) \approx Z_2$ is different from zero if and only if S^{4j-1} is parallelizable.* (Compare Bott and Milnor [5].)

Since S^{4j-1} is parallelizable only for $j = 1, 2$ (see [5] or [6]), it follows that for $j \geqq 3$, the sequence

$$0 \to \boldsymbol{Z}_{(2j-1)!a_j} \xrightarrow{\bar{a}^*} H^{4j+1}(X_{4j-1}) \to H^{4j+1}(X) \to 0,$$

is exact. In order to show that the sequence splits, consider the diagram

$$\begin{array}{ccccccc}
H^{4j}(X) & \xrightarrow{\delta} & H^{4j+1}(X_{4j-1}, X) & \xrightarrow{a^*} & H^{4j+1}(X_{4j-1}) & \to & H^{4j+1}(X) \\
\big\downarrow{\scriptstyle \phi_*} & & \big\downarrow{\scriptstyle \phi_*} & & \big\downarrow{\scriptstyle \phi_*} & & \big\downarrow{\scriptstyle \phi_*} \\
H_2{}^{4j}(X) & \xrightarrow{\delta} & H_2{}^{4j+1}(X_{4j-1}, X) & \xrightarrow{a^*} & H_2{}^{4j+1}(X_{4j-1}) & \to & H_2{}^{4j+1}(X)
\end{array}$$

where $H_2{}^*$ is the cohomology with coefficients in $\mathbf{Z}_2$ and ϕ_* is induced by the coefficient epimorphism $\phi\colon \mathbf{Z}\to\mathbf{Z}_2$. Since $\phi_* u\neq 0$ and δ kills decomposable elements in $H_2{}^{4j}(X)$, it follows that $\phi_*\mathbf{k}^{4j+1}=0$ if and only if $\delta w_{4j}\neq 0$. Hence, by Lemma 6.4 above, $\mathbf{k}^{4j+1}$ cannot be halved unless $j=1$ or 2. Since $H^{4j+1}(X;\mathbf{Z})$ is the direct sum of copies of $\mathbf{Z}_2$, it follows that every element $\neq 0$ in $H^{4j+1}(X;\mathbf{Z})$ is the image of an element *of order two* in $H^{4j+1}(X_{4j-1};\mathbf{Z})$. Thus (6.2′) splits for $j\geqq 3$.

Now, let $j=1$ or 2. Since S^3 and S^7 are parallelizable, it follows that $\delta w_4\neq 0$, $\delta w_8\neq 0$. Thus $\mathbf{k}^5$ and $\mathbf{k}^9$ can be halved. Consider first the case $j=1$: The sequence we are interested in reads

$$H^4(X)\to H^5(X_3,X)\xrightarrow{a^*}H^5(X_3)\to H^5(X)\xrightarrow{\delta'}\cdots.$$

Since $H^5(B_{SO(n)})\approx\mathbf{Z}_2$ generated by W_5, the only possible value of the projection in $H^5(X)$ of $\frac{1}{2}\mathbf{k}^5$ is W_5. Therefore, δ' is trivial also in this case and exactness of (6.2′) holds for $j=1$.

Let $j=2$. Consider the sequence

$$H^8(X)\xrightarrow{\delta}H^9(X_7,X)\xrightarrow{a^*}H^9(X_7)\xrightarrow{p^*}H^9(X)\xrightarrow{\delta'}\cdots.$$

$H^9(B_{SO(n)})\approx\mathbf{Z}_2+\mathbf{Z}_2+\mathbf{Z}_2$ generated by p_1W_5, $(W_3)^3$ and W_9. Let h be an element in $H^9(X_7)$ such that $2h=\mathbf{k}^9$. Claim: $p^*h=W_9+\alpha p_1W_5+\beta(W_3)^3$, where α and β are remainders mod 2 depending on the choice of h. This is equivalent to proving $p^*h\neq\alpha p_1W_5+\beta(W_3)^3$. Since p^* is an isomorphism in dimensions <8, there exist classes p'_1, W'_5, W'_3 whose projection under p^* are p_1, W_5, W_3. Thus $\alpha p'_1W'_5+\beta(W'_3)^3\in H^9(X_7)$ is an element of order 2 whose image by p^* is $\alpha p_1W_5+\beta(W_3)^3$. If p^*h were equal to $\alpha p_1W_5+\beta(W_3)^3$, we would get an element $h'=h-\alpha p'_1W'_5-\beta(W'_3)^3$ with the properties $p^*h'=0$ and $2h'=\mathbf{k}^9$. Such an element however does not exist. It follows from $p^*h=W_9+$ decomposable elements, that $\delta W_9=0$. Hence (6.2′) is seen to be exact in any case.

To obtain the exactness of (6.2″), consider the cohomology sequence

$$H^{8i+s-1}(X)\xrightarrow{\delta}H^{8i+s}(X_{8i+s-2},X)\xrightarrow{a^*}H^{8i+s}(X_{8i+s-2})\xrightarrow{p^*}H^{8i+s}(X)\xrightarrow{\delta'}$$

with coefficients in $\pi_{8i+s-2}(SO(n))\approx\mathbf{Z}_2$ for $s=2$ or 3.

We have to prove that δ and δ' are zero. Since δ and δ' kill decomposable elements, it suffices to prove $\delta w_{8i+1}=0$, $\delta w_{8i+2}=0$, $\delta' w_{8i+2}=0$, $\delta' w_{8i+3}=0$. The first two assertions follow from (5.2), by which

$$\delta w_{8i+s-1}\in H^{8i+s}(X_{8i+s-2},X;\mathbf{Z}_2)\approx\mathbf{Z}_2$$

is the value $\alpha^* w_{8i+s-1}[S^{8i+s-1}]$ of the $(8i+s-1)$-th Stiefel-Whitney class of the $\boldsymbol{SO}(n)$-bundle over S^{8i+s-1} induced by a map representing the generator α of $\pi_{8i+s-1}(B_{\boldsymbol{SO}(n)}) \approx \boldsymbol{Z}_2$. Since such a Stiefel-Whitney class vanishes, it follows that $\delta w_{8i+s-1} = 0$. To prove $\delta' w_{8i+s} = 0$, observe that

$$w_{8i+2} = Sq^2 w_{8i} \text{ for } i \geqq 1, \text{ and } w_{8i+3} = Sq^1 w_{8i+2}$$

(see Wu Wen-Tsün [13] and Borel [1]). It follows that

$$\delta' w_{8i+2} = \delta' Sq^2 w_{8i} = Sq^2 \delta w_{8i} = 0, \text{ and similarly } \delta' w_{8i+3} = 0.$$

The splitting of (6.2″) is trivial since every element in $H^{8i+s}(X_{8i+s-2}; \boldsymbol{Z}_2)$ has order two.

It remains to prove Lemma 6.4. Let ξ' be the associated bundle with fibre $V_{n,n-4j+1} = \boldsymbol{SO}(n)/\boldsymbol{SO}(4j-1)$, and let

$$p_* : H^{4j}(S^{4j}; \pi_{4j-1}(\boldsymbol{SO}(n))) \to H^{4j}(S^{4j}; \pi_{4j-1}(V_{n,n-4j+1}))$$

be induced by $p : \pi_{4j-1}(\boldsymbol{SO}(n)) \to \pi_{4j-1}(V_{n,n-4j+1})$. Identifying $H^{4j}(S^{4j}; \pi_{4j-1}(\boldsymbol{SO}(n)))$ with $\pi_{4j-1}(\boldsymbol{SO}(n)))$, we clearly have $p_*\alpha = w_{4j}(\xi)$, where α is a generator of $\pi_{4j-1}(\boldsymbol{SO}(n))$. Since $\pi_{4j-1}(V_{n,n-4j+1}) \approx \boldsymbol{Z}_2$, it follows that $w_{4j}(\xi)$ is different from zero if and only if $p : \pi_{4j-1}(\boldsymbol{SO}(n)) \to \pi_{4j-1}(V_{n,n-4j+1})$ is surjective. The commutative diagram

$$\begin{array}{ccc} \pi_{4j-1}(\boldsymbol{SO}(4j)) & \to & \pi_{4j-1}(\boldsymbol{SO}(n)) \\ \Big\downarrow p' & & \Big\downarrow p \\ \pi_{4j-1}(S^{4j-1}) & \to & \pi_{4j-1}(V_{n,n-4j+1}) \end{array}$$

shows that p is surjectice if and only if p' is; in other words, if and only if S^{4j-1} is parallelizable.

Remark. The proof in [6] can be improved by using the above diagram from which Lemma 2 of [6] follows immediately.

Proof of Theorem 6.3. Let $X = B_{Sp(n)}$. Again the first statements of the theorem follow trivially from the results of [4].

Consider the exact sequence

$$H^{4j}(X) \xrightarrow{\delta} H^{4j+1}(X_{4j-1}, X) \xrightarrow{a^*} H^{4j+1}(X_{4j-1}) \to H^{4j+1}(X)$$

with integer coefficients ($\pi_{4j}(X) \approx \boldsymbol{Z}$ by [4]).

Since $H^*(B_{Sp(n)}; \boldsymbol{Z}) = \boldsymbol{Z}[K_1, \cdots, K_n]$, $\deg K_j = 4j$, it follows that

$H^{4j+1}(X) = 0$, and the multiples of K_j are the only non-decomposable elements of $H^{4j}(X)$. By (5.2) and Lemma 1.1,

$$\delta K_j = (2j-1)!\, b_j \cdot u,$$

where u is the fundamental class in $H^{4j+1}(X_{4j-1}, X; \mathbf{Z}) \approx \mathbf{Z}$.

It follows that $H^{4j+1}(X_{4j-1})$ is cyclic of order $(2j-1)!\, b_j$ generated by $\boldsymbol{k}^{4j+1}$. The assertions about $\boldsymbol{k}^{8i-1}$ and $\boldsymbol{k}^{8i-2}$ are trivial.

Battelle Memorial Institute, Geneva.

REFERENCES.

[1] A. Borel, "La cohomologie mod 2 de certains espaces homogènes," *Commentarii Mathematici Helvetici*, vol. 27 (1953), pp. 165-197.

[2] ———, *Selected topics in the homology theory of fibre bundles.* Mimeographed Notes, Chicago, 1954.

[3] ——— and F. Hirzebruch, "Characteristic classes and homogeneous spaces, I," *American Journal of Mathematics*, vol. 80 (1958), pp. 458-538; II, vol. 81 (1959), pp. 315-381.

[4] R. Bott, "The stable homotopy of the classical groups," *Proceedings of the National Academy of Sciences*, U. S. A., vol. 43 (1957), pp. 933-935.

[5] ——— and J. Milnor, "On the parallelizability of spheres," *Bulletin of the American Mathematical Society*, vol. 64 (1958), pp. 87-89.

[6] M. Kervaire, "Non-parallelizability of the n-sphere for $n > 7$," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 44 (1958), pp. 280-283.

[7] ———, "On the Pontryagin classes of certain $SO(n)$-bundles over manifolds," *American Journal of Mathematics*, vol. 80 (1958), pp. 632-638.

[8] ———, "Some non-stable homotopy groups of Lie groups," (in preparation).

[9] J. Milnor and M. Kervaire, "Bernoulli numbers, homotopy groups and a theorem of Rohlin," *Proceedings of the International Congress of Mathematicians*, Edinburgh, 1958 (to appear).

[10] F. Peterson, "Some remarks on Chern classes," *Annals of Mathematics* (to appear).

[11] N. Steenrod, *The topology of fibre bundles*, Princeton, 1950.

[12] G. Whitehead, *Homotopy theory*, Mimeographed Notes, M. I. T., 1954.

[13] W. T. Wu, "Les i-carrés dans une variété grasmanienne," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, Paris, vol. 230 (1950), pp. 918-920.

NORMALITY IN SUBSETS OF PRODUCT SPACES.*

By H. H. Corson.

1. **Introduction.** This is a study of the topological properties of some of the subsets of what will be called a Σ-product. For the purposes of this introduction it will be enough to define a Σ-product of copies R_a of the real line where a is in an uncountable index set A. This is the subset Σ of the full product of the R_a which consists of those points which have at most a countable number of non-zero coordinates. The main properties of these spaces are, loosely speaking, strong types of normality and weak types of separability. For instance, it is proved that Σ is not only normal but that the collection of all the neighborhoods of the diagonal in $\Sigma \times \Sigma$ forms a uniformity for Σ. The space Σ is not paracompact or separable although each metric space which is the continuous image of Σ, or is a closed subset of Σ, is separable. Moreover, Σ has a dense subset which is the union of a countable number of compact spaces.

As applications of these theorems, two counterexamples are constructed. First, a normal space is constructed whose real-compactification is not normal. (See Section 3 for the definition of real-compactification.) This question has been asked in a preliminary version of a book by L. Gilman and M. Jerison, and has also been considered elsewhere. Second, it is shown that a space F_0 which was first defined by A. H. Stone (see Section 4) has the property that the collection of all the neighborhoods of the diagonal in $F_0 \times F_0$ forms a complete uniformity for F_0, but F_0 is not paracompact. This answers in the negative a conjecture of Kelley's [9, pages 208-209]. (It is stated that a counterexample had been constructed, but an error was found during a seminar at Purdue.)

Σ is also proved to have the following additional properties. It is a $C(X)$ for a Lindelöf space X, where $C(X)$ is the collection of continuous real functions on X under either the simple topology or the compact open topology—these topologies being the same for this X. Every metric space can be imbedded as a subspace of some Σ-product of real lines. However, it is shown that Σ has a non-normal subset.

* Received December 29, 1958.

Perhaps it is best to mention that in the literature there are a few cases of results on Σ-products of compact spaces X_a, $a \in A$. These are defined by specifying that one point in each X_a is to be 0, and then imitating the above definition of the Σ-product of real lines. These results also follow from the theorems in this paper. However, the reader will see that, for the applications which were described above, it is essential that one consider a Σ-product of non-compact spaces. For the theorems that remain true, most of the proofs given here can be simplified if X_a is compact for each a.

Certain conventions will be followed throughout. A topological space will be a completely regular, Hausdorff space. For a subset F of a topological space X, F^- will be the closure of F in X, while F' will be the complement of F in X.

Finally, some comments of J. R. Isbell are gratefully acknowledged.

2. Normality of Σ-products. Although a Σ-product of real lines was defined in the introduction, it will be possibly usually to deal with a larger class of spaces. These are defined as follows.

Definition. For a collection $\{X_a \colon a \in A\}$ of topological spaces, let $P = P\{X_a \colon a \in A\}$ be the topological product of the X_a. Then a *Σ-product* of the X_a is a subset Σ of P with the property that there exists $p = (p_a) \in P$ such that $q = (q_a) \in \Sigma$ if and only if $q_a \neq p_a$ for at most a countable number of $a \in A$. Such a point p is called the *base point* of this Σ-product.

Perhaps it is best to point out immediately that one Σ-product of the X_a may be different from another if the base point is changed. For instance, suppose that each X_a is a copy of the unit interval $[0,1]_a$ plus an isolated point ∞_a, and let A be uncountable. Then the Σ-product with $p = (\infty_a)$ as the base point is not homeomorphic to that with $p' = (0_a)$ as the base point. In fact, the first space has a point (the base point) whose component is just a single point, while the second Σ-product has no such point.

It will now be proved that a Σ-product of complete, separable metric spaces is normal. The following lemma will be used in the proof, but first some terminology is needed.

Let $\{H_s \colon s \in S\}$ be a collection of subsets of a topological space X, and let U be an open subset of X. It will be said that $\{H_s \colon s \in S\}$ can be separated in U if there is a disjoint collection of open sets $\{U_s \colon s \in S\}$ such that $U \cap H_s \subset U_s$ for all $s \in S$.

LEMMA 1. *Let H_1 and H_2 be two subsets of the product of a topological space Y with a metric space M, and suppose $\mathfrak{U}$ is an open cover of M. If H_1*

and H_2 can be separated in each $Y \times U$, $U \in \mathcal{U}$, then H_1 and H_2 can be separated in $Y \times M$.

Proof. A. H. Stone has proved in [12] that each metric space is paracompact. That is, for each open cover $\mathcal{U}$ of M there is a locally finite refinement $\mathcal{V}$ of $\mathcal{U}$. More explicitly, $\mathcal{V}$ has the property that each $V \in \mathcal{V}$ is contained in some $U \in \mathcal{U}$, and each $x \in M$ has a neighborhood that meets only a finite number of $V \in \mathcal{V}$. Since M is normal, one may even choose V such that the closure of each $V \in \mathcal{V}$ is contained in some $U \in \mathcal{V}$. Let $\mathcal{V}$ be such a refinement for the $\mathcal{U}$ in the statement of Lemma 1.

For each $V \in \mathcal{V}$ there are open sets V_1 and V_2 in $Y \times V$ such that $H_i \cap (Y \times V) \subset V_i$, $i = 1$ or 2, and $V_1 \cap V_2 = \phi$. This is true since H_1 and H_2 can be separated in each $Y \times U$, and hence in $Y \times V$. Since $V^- \subset U$ for some $U \in \mathcal{U}$, one may even assume that $V_1^- \cap H_2 = V_2^- \cap H_1 = \phi$. Let $S_i = \cup\{V_i : V \in \mathcal{V}\}$, $i = 1, 2$. Define $T_1 = S_1 \cap S_2^{-\prime}$, and $T_2 = S_2 \cap S_1^{-\prime}$. Since T_1 and T_2 are open and disjoint, all that is left to prove is that $H_1 \subset T_1$ and $H_2 \subset T_2$.

Let $h \in H_1$, then $h = (y, m)$, where $y \in Y$ and $m \in M$. Choose a neighborhood N of m such that N meets only a finite number of $V \in \mathcal{V}$. Then $Y \times N$ is a neighborhood of h which meets only a finite number of $Y \times V$, and hence only a finite number of V_2. Let $\mathcal{W}$ be this finite collection of V_2. Recall that $V_2^- \cap H_1 = \phi$ for each $V \in \mathcal{V}$. Hence $(\cup \mathcal{W})' \cap (Y \times N)$ is a neighborhood of h which meets none of the V_2. It follows that $H_1 \subset T_1$, and a similar argument shows that $H_2 \subset T_2$.

Remark. Lemma 1 is true for paracompact M, as the proof shows, or more generally for a normal space M and a locally finite cover $\mathcal{U}$ of M. Moreover, if a discrete collection of closed sets $\{H_s : s \in S\}$ is substituted for H_1, H_2, Lemma 1 is still true. Almost the same proof may be used to show this.

THEOREM 1. *A Σ-product of complete metric spaces is normal.*

Proof. Let $\{M_a : a \in A\}$ be a collection of complete metric spaces with ρ_a being a metric on M_a for which M_a is complete. For each finite subset F of A, let $P_F = P\{M_a : a \in F\}$. The metric ρ_F on a subspace of such a P_F will always be taken to be $\rho_F(x, y) = \sup\{\rho_a(x_a, y_a) : a \in F\}$. Henceforth the subscripts on the ρ will be omitted. Also, denote the Σ-product of the M_a by Σ, where the base point of Σ is $p = (p_a)$.

Let H_1 and H_2 be subsets of Σ which cannot be separated in Σ. It will be shown that there are sequences $\{h_i\}$ and $\{k_i\}$ with $h_i \in H_1$, $k_i \in H_2$, and

with $\{h_i\}$ and $\{k_i\}$ converging to the same point in Σ. Hence H_1 and H_2 cannot be closed, disjoint subsets of Σ, and the theorem will follow.

Obviously H_1 and H_2 are not empty since they cannot be separated. Let x_1 be any point in H_1; then there is a countable set of indices C_1 such that $(x_1)_a = p_a$ if $a \notin C_1$. Arrange C_1 in a simple sequence. F_1 will be a finite set of indices which includes the first member of C_1. Put $S_1 = \Sigma$.

Suppose n quadruples (x_i, C_i, F_i, S_i) have been chosen with the following properties: $x_i \in H_1$ for odd i, and $x_i \in H_2$ for even i. Each C_i is a countable set of indices which includes all $a \in A$ such that $(x_i)_a \neq p_a$. Each C_i is arranged in a simple sequence. F_i is a finite set of indices which contains $F_1 \cup \cdots \cup F_{i-1}$ as well as the first i elements of each C_j, $j \leqq i$. Each S_i for $2 \leqq i \leqq n$ is contained in S_j for $j \leqq i$, and S_i satisfies the following condition. If π_i is the natural projection of Σ onto $P_{F_{i-1}}$, then there is a sphere T_i of radius $1/i$ in $P_{F_{i-1}}$ such that $S_i = \pi_{i-1}^{-1}(T_i)$. Moreover, assume that H_1 and H_2 cannot be separated in S_i, and that $x_i \in S_i$. The quadruple for $n+1$ can be chosen as follows.

Let $\mathcal{U}$ be the covering of $M = \pi_n(S_n)$ by spheres of radius $1/(n+1)$. It is easily seen that S_n is homeomorphic to the topological product of M with some topological space, and that M is a metric space. Hence by Lemma 1 there is a sphere T_{n+1} in $\mathcal{U}$ such that H_1 and H_2 cannot be separated in $S_{n+1} = \pi_n^{-1}(T_{n+1})$, because H_1 and H_2 cannot be separated in S_n. In particular, $H_1 \cap S_{n+1}$ and $H_2 \cap S_{n+1}$ are not empty, so one may choose $x_{n+1} \in H_1$ if $n+1$ is odd or $x_{n+1} \in H_2$ if $n+1$ is even. C_{n+1} and F_{n+1} are chosen in the obvious way.

Let $\{h_i\} = \{x_j \colon j \text{ is odd}\}$, and $\{k_i\} = \{x_j \colon j \text{ is even}\}$; it will be shown that $\{h_i\}$ and $\{k_i\}$ converge to the same point in Σ. However, this is equivalent to showing that $\{x_i\}$ converges. In order to establish this last statement, let a be an element of A, but a not in any C_i. In this case $(x_i)_a = p_a$ for all i. If $a \in C_i$ for some i, then $a \in F_n$ for all n sufficiently large. By the definition of the metric on P_{F_n} and by the choice of x_i, $\rho((x_i)_a, (x_j)_a) < 1/n$ for all n sufficiently large and for all i and j greater than n. Hence $\{(x_i)_a\}$ is a Cauchy sequence in M_a, and it follows that $\{x_i\}$ converges to some $x_0 \in P$, the product of the M_a. But $x_0 \in \Sigma$ since $C = \cup\{C_i \colon i = 1, 2, \cdots\}$ is countable, and the proof is complete.

COROLLARY 1. *The product of a countable number of Σ-products of complete metric spaces is normal and countably paracompact.*

Proof. Let X denote this product, and let I be the unit interval. By [5] it is sufficient to prove that $X \times I$ is normal. However, it is obvious that $X \times I$ is simply another Σ-product of complete metric spaces.

Remark. E. Michael has pointed out to me that the proof of Theorem 1 may be used, almost as it stands, to show that Σ is collectionwise normal. That is, a discrete collection of closed subsets of Σ may be separated in Σ. The remark following Lemma 1 was inserted for this reason. Some of Michael's observations have been incorporated into the proofs of Lemma 1 and Theorem 1 so that the statement made above would be easy to verify. However, if each of the metric spaces is also separable, it is proved in Section 4 that Σ has even stronger properties.

3. The real-compactification of a Σ-product. First, a definition and some results given in [8] will be reviewed. "Real-compact" is the same as "Q" in the sense of Hewitt. Specifically, X is *real-compact* if it has the property that, whenever there is a topological space Y and a homeomorphism f of X into a dense subset of Y such that every continuous real function on $f(X)$ can be extended to Y, then $f(X)=Y$. It is proved in [8] that each separable metric space is real-compact, and that a product of real-compact spaces is real-compact. It is also shown that each topological space X can be imbedded as a dense subspace of a real-compact space vX in such a way that each continuous real function on X can be extended to vX. Moreover, vX is unique up to a homeomorphism, and vX is called the *real-compactification* of X.

In the present section, $v\Sigma$ is determined for some Σ-products.

THEOREM 2. *If P is the product of separable metric spaces $\{M_a\colon a\in A\}$, and if Σ is a Σ-product of the M_a, then $P=v\Sigma$.*

Proof. By the above remarks P is real compact. Σ is dense in P. Hence, by the uniqueness of $v\Sigma$, it suffices to prove that every continuous real function on Σ can be extended to P.

If C is a subset of A, let π_C be the natural projection from P to $P_C=P\{M_a\colon a\in C\}$. Speaking loosely, Mazur has proved in [10] that if f is any continuous real function on Σ, then there is a countable set C contained in A and a continuous real function g on P_C such that $f=g\pi_C$. In fact, Σ is a subset of P which is invariant under projection in Mazur's terminology, and all such subsets of P are shown by him to have the above property. It is obvious from this that every continuous real function on Σ can be extended to P.

However, Mazur proves more than is asserted above. He is forced for this reason to assume that, if $\aleph$ is the cardinality of A, then $\aleph$ is less than the first inaccessible cardinal. (See [10] for the definition of this.) This

restriction on A may be avoided here as follows. Bockstein proved in [2] that, given any two disjoint open set U_1 and U_2 in P, there is a countable subset D of A and disjoint open sets V_1 and V_2 in P_D such that $\pi_D(U_i) \subset V_i$, $i=1,2$. His proof may be used to demonstrate the same statement for Σ. Since every continuous real function on Σ is determined by a countable number of pairs of disjoint open sets in Σ, it follows that $f=g\pi_C$ for some countable $C \subset A$. This completes the proof of Theorem 2.

COROLLARY 2. *There is a normal space Σ whose real compactification $v\Sigma$ is not normal.*

Proof. Let Σ be as in Theorem 2 with A uncountable and with each M_a complete but not compact. Then by Theorem 1, Σ is normal. By Theorem 2, $P=v\Sigma$. By a result of A. H. Stone's, P is not normal [12]. (A proof that P is not normal is also given in Section 4.)

4. The neighborhoods of the diagonal in $\Sigma \times \Sigma$. Section 2 contains all the positive results that I know on Σ-products of spaces which are complete metric but not necessarily separable. If each of the factors is separable, however, we have the following theorem.

THEOREM 3. *Let Σ be a Σ-product of complete separable metric spaces $\{M_a\colon a\in A\}$. Then the family of neighborhoods of the diagonal in $\Sigma\times\Sigma$ is a uniform structure for Σ.*

Proof. Let Δ be the diagonal in $\Sigma\times\Sigma$ and U be a fixed neighborhood of Δ. It is sufficient to find a metric space M and a function ϕ from Σ onto M such that $\{(x,y)\colon \rho(\phi(x),\phi(y))<1\}\subset U$. ($\rho$ is the metric in M.)

Some preliminary construction is needed. First observe that Corollary 1 implies that $\Sigma\times\Sigma$ is normal. Δ being closed in $\Sigma\times\Sigma$, there is a continuous function f from $\Sigma\times\Sigma$ to the unit interval such that $f(\Delta)=O$ and $f(U')=1$. It is easy to see that $\Sigma\times\Sigma$ is a Σ-product of $\{M_a\times N_a\colon a\in A\}$, where M_a is homeomorphic to N_a for all $a\in A$. In the proof of Theorem 2 it has been shown that there is a countable subset $C\subset A$ such that $f=g\pi_C$, where π_C is the projection onto $P_C=P\{M_a\times N_a\colon a\in C\}$ and g is a continuous real function on P_C. Let $T_C=P\{M_a\colon a\in C\}$. Clearly, $T_C\times T_C$ may be identified with P_C. Denote by Δ_C the diagonal in $T_C\times T_C$. One see that $\Delta_C=\pi_C(\Delta)$. Let $U_C=\{(x,y)\in T_C\times T_C\colon g(x,y)<1\}$.

The existence of ϕ and M can now be proved as follows. All the neighborhoods of Δ_C in $T_C\times T_C$ do form a uniformity for T_C, since T_C is metric and hence paracompact [9, Theorem 5.27]. It follows that there is

a metric space M and a continuous function ϕ_C from T_C to M such that, in $T_C \times T_C$, $\{(x,y)\colon \rho(\phi_C(x), \phi_C(y)) < 1\} \subset U_C$. Define ϕ to be $\phi_C \sigma_C$, where σ_C is the projection from Σ to T_C.

It will be proved that ϕ has the required property. Let $(x,y) \in \Sigma \times \Sigma$ such that $\rho(\phi(x), \phi(y)) < 1$. Then $\rho(\phi_C(\sigma_C(x)), \phi_C(\sigma_C(y)) < 1$, so $(\sigma_C(x), \sigma_C(y)) \in U_C$ by selection of ϕ_C. Hence $f(x,y) = g\pi_C(x,y) < 1$ by the choice of U_C, and it follows that $(x,y) \in U$ since f is equal to 1 on U'.

COROLLARY 3. *A Σ-product of complete separable metric spaces is collectionwise normal. (See remarks at the end of Section 2 for the definition of collectionwise normality.)*

Proof. It is proved in [3] that collectionwise normality is implied by the property that all the neighborhoods of the diagonal is a uniformity.

The proof of Theorem 3 implies the following additional fact which will be needed.

COROLLARY 4. *If X is a metric space and also a continuous image of a Σ-product of complete separable metric spaces, then X is separable.*

Proof. X is paracompact, since it is metric. Hence for each open cover $\mathcal{V}$ of X there is a neighborhood U of the diagonal in $X \times X$ such that $\{U(x)\colon x \in X\}$ refines $\mathcal{V}$ [9; Theorem 5.28]. If f is a continuous function which maps Σ onto X, then $U_0 = (f \times f)^{-1}(U)$ is a neighborhood of the diagonal in $\Sigma \times \Sigma$. By the proof of Theorem 3 there is a function ϕ from Σ to a metric space M such that $\{(x,y)\colon \rho(\phi(x), \phi(y)) < 1\} \subset U_0$ However, this M is a separable metric space since it is the image of the separable space T_C. Hence there is a countable subset $\{y_i\}$ of Σ such that $\{U_0(y_i)\colon i = 1, 2, \cdots\}$ covers Σ. It follows that $\{U(f(y_i))\colon i = 1, 2, \cdots\}$ covers X, and hence $\mathcal{V}$ has a countable subcover.

Note. There is another proof of Corollary 4 which shows that it remains true for any dense subset of a full product of separable metric spaces.

It is interesting to note that Bockstein's theorem can be used to give a new proof of the theorem [12] that P, the product of an uncountable number of non-compact metric spaces, is not normal. The first part of Stone's proof goes as follows. First note that P has a closed subset P_0 which is homeomorphic to the product of an uncountable number of copies of the integers. Hence it is enough to show that $P_0 = P\{J_a\colon a \in A\}$ is not normal, where J_a is a copy of the integers. Stone then defines two closed subsets F_0 and F_1 of P_0, where F_i is the set of p in P_0 such that, for any given integer $n \neq i$,

$i = 0$ or 1, $p_a = n$ for at most one $a \in A$. It is possible to show very quickly that F_0 and F_1 cannot be separated in P_0. In fact, if F_0 and F_1 could be separated, then there would be a countable subset $C \subset A$ such that $\pi_C(F_0)$ and $\pi_C(F_1)$ could be separated in $P_C = P\{J_a : a \in C\}$, because of Bockstein's theorem [2]. However, given a $C = \{a_j : j = 1, 2, \cdots\}$, the point $p = (p_a) \in P_C$, where $p_{a_j} = j$, is in $\pi_C(F_0) \cap \pi_C(F_1)$.

On the other hand, F_0 as a topological space has some interesting properties itself. In fact, it is a counterexample to the conjecture of Kelley's mentioned in the introduction.

THEOREM 4. *F_0 has the property that the collection $\mathcal{U}$ of all the neighborhoods of the diagonal in $F_0 \times F_0$ forms a complete uniformity for F_0. However, F_0 is not paracompact.*

Proof. Using the notation introduced above, F_0 is a closed subset of P_0, and hence of Σ, the Σ-product of the J_a. Since Σ has the property that the collection of all the neighborhoods of the diagonal forms a uniformity, so does each closed subset. (More generally, it is easy to prove that this property is inherited by closed subsets.) Moreover, F_0 is closed in P_0, and P_0 is complete in the product uniform structure. Hence F_0 is complete in some uniform structure. Consequently F_0 is complete in its strongest uniform structure $\mathcal{U}$ [9, problem 6.L(a)].

In order to show that F_0 is not paracompact, notice the following facts. Since Σ is collectionwise normal by Corollary 3, then each continuous function from the closed subset F_0 of Σ to a Banach space extends to Σ [6]. By Corollary 4, every continuous image M of Σ, where M is metrizable, is separable. Thus the same is true of F_0, since it is well known that each metric space can be imbedded in a Banach space. If F_0 were paracompact, then for each open cover $\mathcal{V}$ there would be a neighborhood U of the diagonal in $F_0 \times F_0$ such that $\{U(x) : x \in F_0\}$ refines $\mathcal{V}$ [9; Theorem 5.28]. But each such U is a member of the strongest uniformity for F_0. Hence there is a metric space M which is the continuous image of F_0 under ϕ, and such that $\{(x, y) : \rho(\phi(x), \phi(y)) < 1\} \subset U$. Since M must be separable, $\mathcal{V}$ has a countable subcover. Hence it follows that if F_0 were paracompact, then it would be Lindelöf. However, consider the open cover of Σ by sets of the form $V_a = \{p \in \Sigma : p_a = 0\}$. Then $\mathcal{V} = \{V_a : a \in A\}$ covers Σ and hence F_0. If $\{V_{a_i} : i = 1, 2, \cdots\}$ is a countable subset of $\mathcal{V}$, then the point $p = (p_a) \in F_0$ is not in any V_{a_i}, $i = 1, 2, \cdots$, where $p_a = 0$, if $a \neq a_i$ and $p_{a_i} = i$. Therefore $\mathcal{V}$ has no countable subcover, F_0 is not Lindelöf, and hence F_0 is not paracompact.

Remark. Since F_0 is closed in Σ, Corollary 1 implies that F_0 is also countably paracompact.

There is another corollary to Theorem 3, which is a known result. If Σ is a non-trivial Σ-product and $\lambda\Sigma$ is any compactification of Σ, then $\Sigma \times \lambda\Sigma$ is not normal. It suffices to prove this in the case where each factor of Σ is a space with exactly two points. However, since the collection of all the neighborhoods of the diagonal is a uniformity for Σ, if $\Sigma \times \lambda\Sigma$ were normal then Σ would be paracompact [4]. Almost the same proof which was used to prove that F_0 is not paracompact may be applied to show that Σ is not paracompact.

It follows from the above remark that a Σ-product of compact spaces need not be normal. However, it is known and easily proved that such Σ are countably compact in this case. As for metric spaces which are not complete, I do not know if a Σ-product of copies of the rational numbers is normal.

5. Metrizable subsets of Σ-products. Σ-products are ordinarily not metrizable or even paracompact, as was mentioned in the introduction. However, the following is true.

PROPOSITION 1. *Every metric space can be imbedded as a subspace of a Σ-product of copies of the unit interval.*

Proof. If M is a metric space, it is shown in [1] that there are a countable number of collections $\mathfrak{A}_i$ of open sets such that $\cup\{\mathfrak{A}_i : i = 1, 2, \cdots\}$ is a basis for M and such that each $\mathfrak{A}_i$ is a discrete collection. (The latter means that each point of M is contained in an open set which meets at most one member of $\mathfrak{A}_i$.) For each i and each A in $\mathfrak{A}_i$, one may choose a countable collection of open sets B_n such that $B_n^- \subset A$ and $A = \cup\{B_n : n = 1, 2, \cdots\}$.

For each B let f_B be a continuous function from M to the unit interval such that $f_B(m) = 1$ if $m \in B$ and $f_B(m) = 0$ if m is not in the A which corresponds to B. For each B let I_B be a copy of the unit interval, and let Σ be the Σ product of the I_B, where the base point is the point which has every coordinate equal to zero. Let ϕ be the function from M to X defined by $(\phi(m))_B = f_B(m)$. It follows from [9, Lemma 4.5] that ϕ is a homeomorphism, which completes the proof.

Remark. On the other hand, if M is a metric space which is a *closed* subspace of a Σ-product of unit intervals, then M must be separable. This follows from the results in Section 4.

6. Non-normal subspaces of Σ-products. Although it has been shown that Σ-products have many normal subspaces, and although more normal subspaces will be exhibited presently, it is nevertheless true that every non-trivial Σ-product has a subset which is not normal. This is easily demonstrated using the next two lemmas.

LEMMA 2. *If X is normal and if A is a subspace of X such that each continuous real function on X is bounded on A, then every sequence in A^- has a cluster point.*

Lemma 2 is known and easily proved. Lemma 3 is due to Melvin Henriksen [7].

LEMMA 3. *Let A be a subspace of X such that every continuous real function on A can be extended to X. Then for $x \in A$, every continuous real function on $A - \{x\}$ can be extended to $X - \{x\}$.*

PROPOSITION 2. *Let Σ be a Σ-product of uncountably many spaces, each having more than one point. Then Σ has a non-normal subset.*

Proof. By hypothesis, each factor X_a of Σ has a two-point subset Y_a. Assume that if $p = (p_a)$ is the base point of Σ then $p_a \in Y_a$. It will be proved that Σ_0 has a non-normal subset, where Σ_0 is the Σ-product of the Y_a with p as base point. Since $\Sigma_0 \subset \Sigma$, Proposition 2 will follow.

Let P_0 be the full product of the Y_a, then $P_0 = v\Sigma_0$ by Theorem 2. Choose some point $q \in P_0$ which is not in Σ_0. Since every continuous real function on Σ_0 can be extended uniquely to P_0, $P_0 - \{q\}$ has the same property with respect to P_0. That is, $P_0 = v(P_0 - \{q\})$. But P_0 is compact, therefore every continuous function on $P_0 - \{q\}$ is bounded. Also, P_0 may be considered to be a topological group and is consequently homogeneous. Hence every continuous function on $P_0 - \{x\}$ is bounded for all x in P_0.

Let x_0 be a fixed point of Σ_0. Lemma 3 implies that each continuous real function on $\Sigma_0 - \{x_0\}$ can be extended to $P_0 - \{x_0\}$. Hence all continuous functions on $\Sigma_0 - \{x_0\}$ are bounded, since $P_0 - \{x_0\}$ has been shown to have this property. However, $\Sigma_0 - \{x_0\}$ contains a sequence with no cluster point. To define this sequence, let x_i be a point in $\Sigma - \{x_0\}$ such that $(x_i)_a \neq (x_0)_a$ for exactly one a. A countable number of distinct a_i has no cluster point. By Lemma 2, $\Sigma_0 - \{x_0\}$ is not normal.

7. A dense Lindelöf subspace of Σ. Suppose Σ is a Σ-product of $\{M_a : a \in A\}$ with base point $p = (p_a)$. Then a *σ-product* of the M_a is the set of $q = (q_a) \in \Sigma$ such that $q_a \neq p_a$ for at most a finite number of a. If σ

is such a σ-product, then $\sigma = \cup\{\sigma_i: i = 0, 1, 2, \cdots\}$, where σ_i is the set of $q = (q_a) \in \sigma$ such that $q_a \neq p_a$ for at most i of the $a \in A$.

LEMMA 4. *If M and each M_a are separable metric, then $\sigma_i \times M$ is Lindelöf.*

Proof. The proof is by induction. It is trivial for $i = 0$, so suppose that the statement is true for σ_n. Let $\mathcal{O}$ be an open cover of $\sigma_{n+1} \times M$. In order to show that there is a countable subcover of $\mathcal{O}$, it may be assumed that each member of $\mathcal{O}$ is a member of the usual product basis for open sets in $\sigma_{n+1} \times M$. Since M is separable metric there is a countable subset of $\mathcal{O}$, say $\{O_i: i = 1, 2, \cdots\}$, which covers $p \times M$, where p is the base point. Since each O_i is a member of the basis, there is a finite subset F_i of A, a neighborhood $V_a{}^i$ of p_a in M_a for each $a \in F_i$, and V^i open in M such that

$$O_i = V^i \times P\{V_a{}^i: a \in F_i\} \times P\{M_a: a \notin F_i\}.$$

Let $G_b{}^i = V^i \times (V_b{}^i)' \times P\{M_a: a \neq b\}$ for each $b \in F_i$; then $G_b{}^i$ is homeomorphic to $V \times (V_b{}^i)' \times \sigma_n$. Since $(V_a{}^i)' \times V^i$ is separable metric, $G_b{}^i$ is covered by a countable number of elements of $\mathcal{O}$. However,

$$\sigma_{n+1} \times M = (\cup\{O_i: i = 1, 2, \cdots\}) \cup (\cup\{G_b{}^i: b \in F_i, i = 1, 2, \cdots\}).$$

Hence $\mathcal{O}$ has a countable subcover.

Lemma 4 is related to a problem of Michael's [11]. He asks if the product of a paracompact space and a metric space is paracompact, but it is even known of the product of a Lindelöf space and a separable metric space is paracompact.

PROPOSITION 3. *The σ-product of separable metric spaces is Lindelöf. Hence each Σ-product of separable metric spaces has a dense Lindelöf subspace.*

Proof. $\sigma = \cup\{\sigma_i: i = 1, 2, \cdots\}$. By Lemma 4, $\sigma_i \times M$ is Lindelöf if M has only one point. Hence σ_i is Lindelöf, and the union of a countable number of Lindelöf spaces is Lindelöf.

8. Σ-products of real lines.

PROPOSITION 4. *Let M_a be homeomorphic to the real line for each $a \in A$. Then σ, the σ-product of the M_a, is the union of a countable number of compact sets*

Proof. Define $(\sigma_i)_j$ to be the set of $p = (p_a) \in \sigma_i$ such that $|p_a| \leq j$ for each $a \in A$. It will suffice to show that $(\sigma_i)_j$ is compact for each i and j. However, it is easy to see that $(\sigma_i)_j$ is closed in the full product $P\{N_a: a \in A\}$,

where N_a is the closed interval $[-j, j]$ contained in M_a. Hence $(\sigma_i)_j$ is compact.

PROPOSITION 5. *Let Σ be a Σ-product of copies of the real line. Then Σ is homeomorphic to $C(X)$, all the continuous real function on a Lindelöf space X, where $C(X)$ has either the simple topology or the compact open topology—these topologies being the same for this X.*

Proof. Let the points in X be the index set A together with a point called ∞. A basis for the open sets in X is defined as follows. Each point of A is open, and complements (in X) of countable subsets of A are open. It is easy to see that Σ is homeomorphic to $C_0(X)$, the functions in $C(X)$ which vanish at ∞. However, $C(X)$ is homeomorphic to $C_0(X) \times R$, where R is the real line, which is in turn homeomorphic to $\Sigma \times R$. If A is infinite, then $\Sigma \times R$ is homeomorphic to Σ, while the proposition is obvious if A is finite.

REFERENCES.

[1] R. H. Bing, "Metrization of topological spaces," *Canadian Journal of Mathematics*, vol. 3 (1951), pp. 175-186.

[2] M. Bockstein, "Un théorème de séparabilité pour les produits topologiques," *Fundamenta Mathematicae*, vol. 35 (1948), pp. 242-246.

[3] H. J. Cohen, "Sur un problème de M. Dieudonné," *Comptes Rendus Hebdonaires des Séances de l'Academie des Sciences*, vol. 234 (1952), pp. 290-292.

[4] H. H. Corson, "The determination of paracompactness by uniformities," *American Journal of Matematics*, vol. 80 (1958), pp. 185-190.

[5] C. H. Dowker, "On countably paracompact spaces," *Canadian Journal of Mathematics*, vol. 3 (1951), pp. 219-224.

[6] ———, "On a theorem of Hanner," *Arkiv för Matematik*, vol. 2 (1952), pp. 307-313.

[7] Melvin Henriksen, "On minimal completely regular spaces associated with a given ring of continuous functions," *The Michigan Mathematical Journal*, vol. 4 (1957), pp. 61-64.

[8] Edwin Hewitt, "Rings of real-valued continuous functions I," *Transactions of the American Mathematical Society*, vol. 64 (1948), pp. 45-99.

[9] John L. Kelley, *General Topology*, New York, 1955.

[10] S. Mazur, "On continuous mappings on Cartesian products," *Fundamenta Mathematicae*, vol. 39 (1952), pp. 229-238.

[11] E. Michael, "A note on paracompact spaces," *Proceedings of the American Mathematical Society*, vol. 4 (1953), pp. 831-838.

[12] A. H. Stone, "Paracompactness and product spaces," *Bulletin of the American Mathematical Society*, vol. 54 (1948), pp. 977-982.

ERRATA TO OUR PAPER "LOCAL UNIQUENESS, ETC." *

(this Journal, vol. 80, pp. 421-430.)

By Fred Brauer and Shlomo Sternberg.

A number of errors occur in our paper which we should like to rectify. In Theorem 1 we give a uniqueness criterion which we state is sufficiently general so as not to imply the convergence of successive approximations. We show this in Section 4 by giving the Müller example as an instance of a differential equation which satisfies our criterion but for which the successive approximations do not converge. The statement is true but the proof that we give there does not make any sense. The argument should proceed as follows. We first prove that our criterion implies the following well known lemma.

Let $f(x,t)$ be a continuous function which is monotone non-increasing in x for all $0 \leqq t \leqq a$. Then the differential equation $dx/dt = f(x,t)$, $x(0) = 0$ has unique solution on $0 \leqq t \leqq a$.

The proof of this lemma is obtained by taking $V(x,t)$ to be x^2. Then (4) becomes

$$2(x-y)[f(x,t)-f(y,t)] \leqq \omega(V,t)$$

which is satisfied with $\omega = 0$. Since the Müller example satisfies the hypotheses of the lemma, we are done. It may be of some interest that the above criterion is a consequence of our theorem. It is not a consequence of Kamke's "allgemeine Eindeutigkeitssatz."

The results of Section 6, where we attempt to impose additional conditions to guarantee the convergence of successive approximations contain errors of a more serious nature. Our proof of Theorem 4 is incomplete, and it is not clear at the moment whether or not the theorem is true. The conclusion is correct if one imposes the additional hypothesis that V obeys the inequality $V(x+y, \max(t_1,t_2)) \leqq V(x,t_1) + V(x,t_2)$. Even so, the monotonicity condition on $\omega(r,t)$ seems to be indispensable.

We should like to thank Professors J. Dieudonné, P. Hartman, and J. P. LaSalle for calling these errors to our attention.

* Received May 21, 1959.

THEORY OF INFINITE DERIVATIVES.*[1]

By LEON EHRENPREIS.

Introduction. We shall study here an extension of the theory of distributions of L. Schwartz (see Schwartz [1]) so as to include linear functions on spaces of analytic functions. Such an extension has been discussed from a different point of view in Ehrenpreis [1], [2]. The main viewpoint of the present paper is the following: Let R denote the real axis, and let $a=\{a_i\}$ be a sequence of complex numbers. We shall say that the indefinitely differentiable function f on R is in the domain of $(d/dx)^a$ if the series

$$\sum a_i(d^if/dx^i)$$

converges in a certain sense. We say that the continuous function g on R is in the domain of X^a if the series

$$\sum a_ix^ig(x)$$

converges in a suitable sense. The Fourier transform (formally) maps the set of functions in the domain of $(d/dx)^a$ onto the set of functions in the domain of X^a.

Now, let A be a class of sequences of complex numbers. Call K the space of functions which are in the domain of $(d/dx)^a$ for all $a\in A$, so K is a space of analytic or quasi-analytic or non quasi-analytic functions. Call L the space of functions in the domain of X^a for all $a\in A$, so L is a space of functions which have a certain growth property at infinity. Then the Fourier transform (formally) maps K onto L. Thus, we have a characterization of the Fourier transform of classes of analytic or quasi-analytic or non-quasi-analytic functions. Conversely, the above provides a method of characterizing the Fourier transform of spaces of functions determined by growth conditions.

By means of the operators $(d/dx)^a$, X^a, we give natural topologies to the spaces K, L. K', the dual of K, is a space of continuous linear functions on a space of analytic or quasi-analytic or non quasi-analytic functions. In general, the space $\mathcal{D}$ of Schwartz (see Schwartz [1]) is not dense in K, so

* Received September 12, 1958.

[1] Work partially supported by National Science Foundation Grants NSF 5-G 205 and NSF 5-G 1010.

that K' cannot be identified with a space of distributions. In particular, there will not, in general, exist partitions of unity in K (or K'). However, for most of the applications of our theory to partial differential equations and to integral equations, we do not need to use partitions of unity, but rather the most important object to be studied is the Fourier transform of K'; our theory is developed specifically for this purpose.

There are two essential parts to our paper. Part I deals with spaces which are defined by both growth conditions at infinity and regularity. We study some of the subspaces of the space $\mathcal{D}$ of Schwartz [1] which are of importance in refined studies of hyperbolic partial differential equations and integral equations (see Ehrenpreis [10]). For these spaces we discuss explicitly the Fourier transform.

In part II we are concerned with spaces which are defined only by regularity conditions. We study the space of functions analytic on an arbitrary set in the plane. A topology for these spaces of analytic functions has already been given by Van Hove (see Van Hove [1], Waelbroeck [1]) but, except for some special cases, we do not know whether or not our topology is the same as the Van Hove topology.

Our notations and proofs cover only the case of dimension one, but it is easy to extend the methods to higher dimensions. In particular, we are able to give a natural definition to the Fourier transform on an analytic variety imbedded in euclidean space.

I. Spaces of infinitely differentiable functions. Let R denote the real axis, and let $a = \{a_i\}$ be a sequence of complex numbers. We shall say that the function f on R is in the domain of D^a if f lies in the space $\mathcal{S}$ of Schwartz (see Schwartz [1]) and if, for any k, the series $\sum a_i(d^i/dx^i)X^kf$ converge in the space $\mathcal{S}$, where X is the function on R: $X(x) = x$. If this is the case we set $D^af = \sum a_i(d^i/dx^i)f$. We say that g is in the domain of X^a if $g \in \mathcal{S}$ and for any k the series $\sum a_iX^ig^{(k)}$ converges in $\mathcal{S}$. If this is the case, we set $X^ag = \sum a_iX^ig$.[2] The existence of a non-zero function g in the domain of X^a (and hence also of D^a) is clearly equivalent to the analyticity of $a(z) = \sum a_jz^j$ at $z = 0$.

[2] We have used the space $\mathcal{S}$ as the base space in our definition of infinite differentiation and infinite multiplication because we shall be most concerned with studying the behavior of functions in the domains of X^a and D^a under Fourier transform, and the Fourier transform is a topological isomorphism of $\mathcal{S}$ onto $\mathcal{S}$ (see Schwartz [1]). Actually, later on, we shall consider other types of infinite differential operator in which, for example, the use of the space $\mathcal{S}$ in the definition of D^a is replaced by that of the space $\mathcal{E}$ of Schwartz (see Schwartz [1]).

When we speak of a class C of sequences, we shall mean a class of sequences $b=\{b_i\}^{\infty}_{i=0}$ of complex numbers such that all sequences in which all but a finite number of terms are different from zero belong to C. Let $\Gamma=C_1,C_2,\cdots,L_1,L_2,\cdots$, where the C_i and L_i are classes of sequences. The space $\mathcal{S}_\Gamma$ is defined as consisting of all functions f with the following property: For any $r\geqq 1$, let a_i be a sequence in C_i and b_i a sequence in L_i for $i=1,2,\cdots,r$; then f is in the domain of $X^{b_r}D^{a_r}\cdots X^{b_1}D^{a_1}$. By the linearity of X^a and D^a we see that $\mathcal{S}_\Gamma$ (which we shall usually denote by $\mathcal{S}$ if no confusion is possible) is a vector space over the complex numbers, which may, of course, be reduced to $\{0\}$. In $\mathcal{S}$ we introduce a locally convex topology by means of the semi-norms

$$v_{c,d,c',d';a_1,a_2,\cdots,a_r,b_1,b_2,\cdots,b_r}(f)$$
$$=\sup_{x\in R}|((d^c/dx)X^dX^{b_r}D^{a_r}\cdots X^{b_1}D^{a_1}(d^{c'}/dx)X^{d'}f)(x)|$$

for all positive integers r,c,d,c',d' and all sequence $a_i\in C_i$ and $b_i\in L_i$ for $i=1,2,\cdots,r$. Since all sequences in which only a finite number of non-zero terms appear belong to each C_i and L_i, it is immediate that $\mathcal{S}$ is Hausdorff. On the other hand, $\mathcal{S}$ need not be metrizable as a later example will show.

PROPOSITION 1. *Suppose the sets L_j, C_j have the property that, if the sequence $\{a_l\}$ belongs to any of them, then so does $\{\epsilon_l a_l\}$ whenever $|\epsilon_l|=1$ for all l. Suppose that for every k, $\{C_k{}^l a_l\}\in L_j$* (or C_j) *whenever $\{a_l\}\in L_j$* (or C_j). *Then $\mathcal{S}$ is complete.*

Proof. Let Q be any operator of the form $X^{b^r}D^{a^r}\cdots X^{b^1}D^{a^1}$, where, for each j, $b^j\in L_j$, $a^j\in C$, and let f lie in the closure of $\mathcal{S}$; we must show that f is in the domain of Q. An easy induction reduces the general case to the cases where $r=1$ and either D^{a^1} or $X^{b^1}=$ identity. By Fourier transform we may assume that $D^{a^1}=$ identity. Then we can find functions f^j in the domain of X^{b^1} such that $\{X^{b^1}f^j\}$ converges in the topology of $\mathcal{S}$, and, for any $l\geqq 0$. $X^lf^j\to X^lf$ in the topology of $\mathcal{S}$. Let $b^1=\{b_k\}$, $b=\{|b_k|\}$, $b'=\{(-1)^k|b_k|\}$. By our hypotheses, we may assume that $\{X^bf^j\}$ and $\{X^{b'}f^j\}$ converge in the topology of S. Let

$$B(z)=\sum|b_k|z^j,\qquad B'(z)=\sum|b_k|(-z)^k.$$

We claim first that Bf and $B'f$ are bounded functions on R. To see this, we know that $\{Bf^j\}$ converges uniformly on R. For any $x\in R$, we must have $B(x)f^j(x)\to B(x)f(x)$ because $f^j(x)\to f(x)$. Since $\{B(x)f^j(x)\}$ converges uniformly on R, it follows that $B(x)f(x)$ is uniformly bounded on R.

Call $\beta(z)=\sum|b_l||\delta_l|z^l$, where $\delta_l=C_2^{l+1}=l(l+1)/2$ so $\sum 1/\delta_l<\infty$, $\beta^1(z)=\sum|b_l\delta_l|(-1)^l z^l$. So βf and $\beta^1 f$ are bounded on R (and even lie in $\mathcal{S}$). Then since the coefficients of β are bounded, we can find an M so that for all $x\geqq 0$, and all l,

$$|b_l x^l \delta_l f(x)|\leqq M=\max_{x\geqq 0}|\beta(x)f(x)|,$$

that is

$$|b_l x^l f(x)|\leqq M/\delta_l.$$

This means that $\sum b_l x^l f(x)$ converges uniformly for $x\geqq 0$ (and similarly for $x\leqq 0$). Thus, $\sum b_l X^l f$ converges uniformly on R.

Now, for any k, we must show that $\sum b_l(d^k/dx^k)(X^l f)$ converges uniformly on R. We use induction on k; for $k=0$, the result is proven above. Assume $k>0$ and that the result is proven for derivatives of lower order. Then we have

$$\sum b_l(d^k/dx^k)X^l f=\sum b_{l,p}X^{l-p}f^{(p)},$$

where $b_{l,p}=C_p^{l+p}b_l$. Now, for each p, $\{b_l^p\}=\{b_{l+p,p}\}\in L^1$. Thus, by the result for $k=1$, $\sum_l b_{l,p}X^{l-p}f^{(p)}$ converges uniformly on R. Thus, $\sum b_l(d^k/dx^k)X^l f$ converges uniformly on R.

By similar reasoning we find that, for any $r\geqq 0$, $k\geqq 0$,

$$\sum(1+x^r)b^l(d^k/dx^k)(X^l f)$$

converges uniformly on R. This implies that $\sum b_l x^l f$ converges in $\mathcal{S}$. This means that f is in the domain of Q and so concludes the proof of Proposition 1.

Problem. Is it true that, for the space $\mathcal{S}$, the condition $\sum h_l$ converges in $\mathcal{S}$ implies, for any k, $\sum|(d^k/dx^k)h_l|$ converges uniformly on R? If this is the case, then the additional hpothesis $\{C_k^l a_l\}\in L_j$ (or C_j) is not necessary as is easily seen.

The space $\hat{\mathfrak{G}}_\Gamma$ (or $\hat{\mathfrak{G}}$) is defined as consisting of all functions in the domain of $D^{a_r}X^{b_r}\cdots D^{a_1}X^{b_1}$ for any positive integer r and any sequences $a_i\in C_i$, $b_i\in L_i$ for $i=1,2,\cdots,r$. It is clear that $\hat{\mathfrak{G}}$ is a vector space over the complex numbers. The topology of $\hat{\mathfrak{G}}$ is defined by means of the seminorms

$$u_{c,d,c',d';b_1b_2,\cdots,b_r,a_1,a_2,\cdots,a_r}(f)$$
$$=|\sup_{x\in R}((d^c/dx)X^d D^{b_r}X^{a_r}\cdots D^{b_1}X^{a_1}(d^{c'}/dx)X^{d'}f)(x)|$$

for $f\in G$, all positive integers r,c,d,c',d' and all $a_i\in C_i$, $b_i\in L_i$ for $i=1,2,\cdots,r$. It is clear that, given any Γ, we can find a Γ' and a Γ'' so that

$\mathfrak{G}_{\Gamma} = \hat{\mathfrak{G}}_{\Gamma'}$, $\hat{\mathfrak{G}}_{\Gamma} = \mathfrak{G}_{\Gamma''}$. Thus, the same remarks on the topology of the space $\mathfrak{G}$ apply to the space $\hat{\mathfrak{G}}$.

PROPOSITION 2. *G is a Montel space, that is, the closed bounded sets of G are compact.*

Proof. For every $f \in \mathfrak{G}$ we associate the system $\{Qf\}$, Q being any operator of the form $X^{b_r}D^{a_r} \cdots X^{b_1}D^{a_1}$ for $a_i \in C_i$, $b_i \in L_i$. The set of these systems $\{Qf\}$ for $f \in \mathfrak{G}$ may be thought of as a vector space V of continuous mappings of R into a space W which is a Cartesian product of the complex plane with itself a certain (in general, a non-denumerable) number of times. Now, if V is given the topology of uniform convergence on R (that is, a fundamental system of neighborhoods of zero in V consists of those sets N for which we can find a neighborhood M of zero in W so that N consists of those $g \in V$ with $g(x) \in M$ for all $x \in R$) then it is easily seen that $f \to \{Qf\}$ is a topological isomorphism of G onto V.

Let B be a bounded set in V. Then it is immediate that the set $\{(d/dx)Qf\}$ for $\{Qf\} \in B$ is again bounded in B. This implies that $x \to \{(Qf)(x)\}$ are, for $x \in R$, equicontinuous maps of R into W. Thus, by the theorem of Ascoli (see Bourbaki [1]) B is relatively compact (that is, the closure of B is compact) in V. Thus, V and hence $\mathfrak{G}$ is a Montel space.

By similar reasoning, we could show that $\mathfrak{G}$ is even a Schwartz space (see Grothendieck [1]).

By dx we shall denote the usual Lebesgue measure on R divided by 2π. Then we define the Fourier transform $\mathfrak{F}$ on $\mathfrak{G}$ by

$$(\mathfrak{F}(f))(x) = \int f(y) \exp(-ixy)\, dy$$

for any $f \in G$, $x \in R$, where unless otherwise specified, all integration will be taken over R. It is clear that the above integral converges uniformly for $x \in R$ and, in fact, we can easily verify from the theory of integration (see Bourbaki [2]) and the fact that the Fourier transform is a topological isomorphism of $\mathfrak{S}$ onto $\mathfrak{S}$:

THEOREM 1. *$\mathfrak{F}$ is a topological isomorphism of $\mathfrak{G}$ onto $\hat{\mathfrak{G}}$.*

We shall usually use lower case letters for elements of $\mathfrak{G}$ and the corresponding upper case letter for their Fourier transforms.

Let A be a topological vector space (by "vector space," we shall always mean "vector space over the complex numbers"); by A' we denote the dual of A with the topology of uniform convergence on the compact sets of A. In case that A is a Montel space, this topology is the same as that of uniform

convergence on the bounded sets of A. For $a' \in A'$, $a \in A$, we shall usually write $a' \cdot a$ for $a'(a)$.

Let B be another topological vector space and $L\colon A \to B$ a continuous linear or anti-linear map. Then we define the *adjoint* L' of L (see Ehrenpreis [6]) as the continuous linear (anti-linear) map of $B' \to A'$ by

$$L'b' \cdot a = b' \cdot La \qquad \text{for } L \text{ linear}$$

$$L'b' \cdot a = \overline{b' \cdot La} \qquad \text{for } L \text{ anti-linear}$$

for any $a \in A$, $b' \in B'$, where for any complex C, $\bar{C}$ is its conjugate.

The elements of $\mathfrak{G}'$ (or $\hat{\mathfrak{G}}'$) *are called hyperdistributions.* If Q is any operator of the form $X^{b_r}D^{a_r} \cdots X^{b_1}D^{a_1}$ with $a_j \in C_j$, $b_j \in L_j$, then Q may be thought of as defining the continuous lienar map $f \to Qf$ of $\mathfrak{G} \to \mathfrak{S}$. By Q' we denote the adjoint of this map.

Let us denote by Z the Banach space of functions which are continuous and bounded on R and zero at infinity with the norm $\| f \| = \max\limits_{x \in R} | f(x) |$ for $f \in Z$. We call an element of Z' a *bounded measure.* Any $u \in Z'$ may be identified with the hyperdistribution (which we again denote by u): $f \to \int f\, du$.

PROPOSITION 3. *For any $S \in \mathfrak{G}'$, we can find a finite sequence of bounded measures $u_1, \cdots, u_s$ and a corresponding sequence of operators $Q_1, \cdots, Q_s$ of the form $X^{b_r}D^{a_r} \cdots X^{b_1}D^{a_1}$ with $a_i \in C_i$, $b_i \in L_i$ such that*

$$S = \sum Q'_i u_i. \tag{1}$$

Proof. S is bounded on some neighborhood of zero in $\mathfrak{G}$. Thus we can find operators $Q_1, \cdots, Q_s$ of the form as described above such that the conditions $f \in G$, $\max\limits_{x \in R} | (Q_i f)(x) | \leqq 1$ imply $| S \cdot f | \leqq 1$. We may clearly suppose, without loss in generality, that Q_1 is the identity operator.

To each $f \in \mathfrak{G}$ we associate the system $\{Q_i f\}$. Then $f \to \{Q_i f\}$ is a linear one-one map of $\mathfrak{G}$ onto a set Y which is a vector subspace of Z^s (the cartesian product of Z with itself s times). Let us give Z^s the topology of a cartesian product space, and Y the topology induced by Z^s. Then the formula

$$L \cdot \{Q_i f\} = S \cdot f$$

defines L as a continuous linear function on Y. Thus, by the Hahn-Banach theorem, L can be extended to a continuous linear function T on Z^s. Since the dual of a cartesian product is the direct sum of the duals, and since the dual of Z is the space of bounded measures, we can find bounded measures $u_1, \cdots, u_s$ so that, for any $\{v_i\} \in Z^s$,

$$T \cdot \{v_i\} = \sum u_i(v_i).$$

In particular, for $f \in \mathcal{G}$,

$$
\begin{aligned}
S \cdot f &= L \cdot \{Q_i f\} \\
&= T \cdot \{Q_i f\} \\
&= \sum u_i \cdot Q_i f
\end{aligned}
$$

which is the desired result.

By c we denote the map of $\mathcal{G} \to \mathcal{G}'$: $cf \cdot g = \int \bar{f}(x) g(x)\, dx$ for any $f, g \in G$. The map ℓ is defined similarly for the space $\hat{\mathcal{G}}$. It is clear that c and ℓ are continuous. Moreover, for any $f \in \mathcal{G}$, $h \in \mathcal{G}$, $\ell h \cdot h > 0$ and $cf \cdot f > 0$ so that c and ℓ are one-one.

PROPOSITION 4. *$c(\mathcal{G})$ is dense in $\mathcal{G}'$.*

Proof. It is sufficient to show that every element of $\mathcal{G}''$ which is zero on $c(\mathcal{G})$ is zero on $\mathcal{G}'$. Let them $L \in \mathcal{G}''$ be zero on $c(\mathcal{G})$. By the thecrem of Mackey and Arens (see Mackey [1], [2], Arens [1], Dieudonné and Schwartz [1]), there is a $g \in G$ so that, for any $S \in {}'\mathcal{G}$, $LS = S \cdot g$. In particular, $0 = L(cg) = cg \cdot g = \int |g(x)|^2\, dx$. Thus, $g = 0$ which means $L = 0$; this is what was to be proven.

Let us denote by $\hat{\mathcal{F}}$ the adjoint of $\mathcal{F}^{-1}$. By the usual Plancherel theorem (see Titchmarsh [2]), for any $f, g \in \mathcal{G}$,

$$\hat{\mathcal{F}} cf \cdot G = cf \cdot g = \ell \mathcal{F} f \cdot G.$$

Thus, $\hat{\mathcal{F}} cf = \ell \mathcal{F} f$ which makes it natural to call $\hat{\mathcal{F}}$ the Fourier transform on $\mathcal{G}'$. (In the terminology of Ehrenpreis [6], $\mathcal{F}$ is (c, l) unitary.) From Theorem, 1, we deduce immediately

THEOREM 2. *$\mathcal{F}$ is a topological isomorphism of $\mathcal{G}'$ onto $\hat{\mathcal{G}}'$. In fact, $\hat{\mathcal{F}}^{-1} = \mathcal{F}'$.*

We shall need several lemmas for the following examples; the first lemma is due to Poincaré [1].

LEMMA 1. *Let f be any continuous function on R. Then there exists an entire function h such that $h(x) \geqq |f(x)|$ for all $x \in R$.*

Proof. Lemma 1 will be proven if we can show the following: Given any sequence $\{a_n\}$ of positive numbers, we can find a sequence $\{h_n\}$ of non-negative numbers so that $h(z) = \sum h_n z^{2n}$ is entire and $h(j) \geqq a_j$ for all j. Let us consider the function $h(z) = \sum a_n (z/n)^{b_n}$, where the even integers b_n are chosen so large that h is entire. It is readily verified that this can be done. Then h has the desired properties and Lemma 1 is proven.

LEMMA 2. *Let $a=\{a_j\}$ be an infinite sequence with the property that $i^j a_j \geqq 0$ for all j; set $a'=\{a_j'\}$, where $a_j'=(-1)^j a_j$. Suppose that f is in the domain of D^a, and*

$$|((d^k/dx^k)D^a f)(x)| \leqq 1/16(1+x^2) \quad \textit{for } k=0,1,2.$$

for all $x \in R$ with a similar inequality for $D^{a'}f$ in place of $D^a f$. Then we also have $|a_j f^{(j)}(x)| \leqq 1$ for all j, and all $x \in R$.

Proof. If F denotes the inverse Fourier transform of f, then by our hypotheses we have for all $x \in R$

$$|\sum |a_j| x^j F(x)| \leqq 1/4(1+x^2)$$

and

$$|\sum |a_j| (-1)^j x^j F(x)| \leqq 1/4(1+x^2).$$

Thus, for any $x \in R$, and any j,

$$|a_j x^j F(x)| \leqq 1/4(1+x^2).$$

This gives immediately the desired result.

Definition. For any sequence $a=\{a_j\}$ for which no $a_j=0$, we call $a^*=\{1/j!a_j\}$ the *polar sequence* of a. If h is an analytic function at 0, $h(z)=\sum h_j z^j$, with no $h_j=0$, then $h^*(z)=\sum z^j/h_j j!$ is called the *polar polar function* of h (if it is analytic at 0).

LEMMA 3. *Given any entire function h, where $h(z)=\sum h_j z^j$, there exists an entire function h' with $h'(z)=\sum h_j' z^j$, where, for each j, $h_j' \geqq 0$, and $h_j' \geqq |h_j|$, and the polar function h'^* of h' is entire.*

Proof. For each $j \geqq 0$, set $k_j = \sup_{l \geqq j} |h_l|$; it is clear that $\{k_j\}$ is monotonically decreasing and that $K(z)=\sum k_j z^j$ is entire. Next, define $h_j' = \max(k_j, 1/\Gamma(j/2))$. Then clearly $h_j' \geqq |h_j|$ for all j. Moreover, $h_j'^* \leqq \Gamma(j/2)/j!$; it follows easily that both h' and h'^* are entire.

LEMMA 4. *Let f be any continuous function on R such that, for each $c>0$ we can find $\eta>0$ with $e^{c|x|} \leqq \eta f(x)$ for all $x \in R$. Then we can find an entire function h such that the polar function h^* of h is entire and such that*

$$f(x) \geqq \begin{cases} h(x) & \textit{for } x \geqq 0 \\ h(-x) & \textit{for } x \leqq 0. \end{cases}$$

Proof. We may clearly assume that f is monotonically increasing for $x \geqq 0$, $f(x)=f(-x)$, and that $f(x) \geqq e^x$ for all x. For each integer $l>1$,

we choose a positive number e_l such that $f(x) \geqq 2e^{lx}$ for $x \geqq e_l$. (The existence of such an e_l is guaranteed by the hypotheses of Lemma 4.) Next, for each $l > 1$ we choose a positive integer d_l such that

$$\sum_{j \geqq d_l} l^j x^j / j! \leqq e^{(l-1)x} / 2^l \text{ for } x \leqq e_l.$$

(The existence of d_l is obvious.) We define $h(z) = \sum h_j z^j$ by: $h_j = l^j/j!$ for $j = d_l, d_l + 1, \cdots, d_{l+1} - 1$, where $d_1 = 0$.

It is clear that for any l the series $\sum h_j \,|\, x \,|^j$ converges uniformly for $|\, x \,| \leqq e_l$, so that $h(z) = \sum h_j z^j$ is entire. That h^* is entire is obvious. Finally, for any $l > 1$, if $e_{l-1} \leqq x\, e_l$ (where $e_1 = 0$)

$$\begin{aligned} |\, h(x) \,| &\leqq \sum h_j \,|\, x \,|^j \\ &\leqq \sum_{j < b_l} (l-1)^j |\, x \,|^j / j! + \sum_{k \geqq l} \sum_{j \geqq b_k} k^j \,|\, x \,|^j / j! \\ &\leqq e^{(l-1)|x|} + \sum_{k \geqq l} e^{(l-1)|x|} / 2^k \\ &< 2e^{(l-1)|x|} \\ &\leqq f(e_{l-1}) \\ &\leqq f(x). \end{aligned}$$

This completes the proof of Lemma 4.

LEMMA 5. *Let* $\{a_j\}$ *be a sequence of complex numbers such that* $\sum a_j z^j$ *is an entire function and* $i^j a_j \geqq 0$ *for all* j; *let* $f \in S$. *Suppose that*

$$\max_{x \in R} (1 + x^2) \,|\, \sum a_j f^{(j)}(x) \,| \leqq \tfrac{1}{2}, \quad \max_{x \in R} (1 + x^2) \,|\, \sum (-1)^j a_j f^{(j)}(x) \,| \leqq \tfrac{1}{2}$$

and

$$\max_{x \in R} (1 + x^2) \,|\, \sum a_j f^{(j+2)}(x) \,| \leqq \tfrac{1}{2}, \quad \max_{x \in R} (1 + x^2) \,|\, \sum (-1)^j a_j f^{(j+2)}(x) \,| \leqq \tfrac{1}{2},$$

where we assume that the series $\sum a_j f^{(j)}$, $\sum (-1)^j a_j f^{(j)}$, $\sum a_j f^{(j+2)}$, $\sum (-1)^j f^{(j+2)}$ *converge in* $\mathcal{S}$. *Then we have*

$$\max_{x \in R} \sum |\, a_j f^{(j)}(x) \,| \leqq 1.$$

Proof. Call $A(z) = \sum |\, a_j \,|\, z^j$ and $A'(z) = \sum (-1)^j \,|\, a_j \,|\, z^j$. Then our hypotheses imply that

$$\begin{aligned} |\, A(x) F(x) \,| &\leqq \tfrac{1}{2}, \qquad |\, A(x) x^2 F(x) \,| \leqq \tfrac{1}{2}, \\ |\, A'(x) F(x) \,| &\leqq \tfrac{1}{2}, \qquad |\, A'(x) x^2 F(x) \,| \leqq \tfrac{1}{2}, \end{aligned}$$

for any $x \in R$. Thus,

$$(1 + x^2) A(|\, x \,|) \,|\, F(x) \,| \leqq 1$$

for all $x \in R$. This means that

$$\max_{x \in R}(1+x^2)\sum |a_j|\,|x|^j\,|F(x)| \leqq 1.$$

Now, we clearly have, for any $y \in R$,

$$|f^{(j)}(y)| \leqq \int |x^j F(x)|\, dx$$

so that

$$\begin{aligned}\sum |a_j f^{(j)}(y)| &\leqq \sum |a_j| \int |x^j F(x)|\, dx \\ &= \int \sum |a_j x^j F(x)|\, dx \\ &\leqq \int (1+x^2)^{-1} dx \\ &< 1\end{aligned}$$

because dx is the usual Lebesgue measure divided by $(2\pi)^{\frac{1}{2}}$. The interchange of summation and integration above is justied because all the terms are positive.

Remark. It is very curious that we need the Fourier transform to prove Lemma 5. Actually, it should be possible to give a direct proof of the lemma without using Fourier transform, but we have not been able to accomplish this.

LEMMA 6. *Let $l < 1$ and let β be any positive function on R such that for all $\epsilon > 0$, $\beta(x) = O(\exp(|x|^{l+\epsilon}))$. Then we can find an entire function B of order l such that $B(z)$ has positive Taylor coefficients at zero, $B(0) \geqq 1$, and $B(x) \geqq \beta(x)$ for $x \geqq 0$, and if $B(x) = \sum b_j x^j$, then $jb_j \leqq b_{j-1}$.*

Proof. Let n_0 be the smallest integer $\geqq 1$ so that $l + 1/n_0 < 1$. Choose $C \geqq 1$ so that

$$\beta(x) \leqq C \sum x^j/\Gamma(j/(l+1/n_0)+1) \text{ for } x \geqq 0.$$

(For the existence of C and the other constants to be defined below, cf. Lemma 13 below.) For each $n \geqq n_0$, we define d_n as the smallest number $\geqq 1$ (and $\geqq d_{n-1}$ for $n > n_0$) for which

$$\beta(x) \leqq \sum x^j/\Gamma(j/(l+1/n)+1) \text{ for } x \geqq d_n - 1.$$

Next we define e_{n_0} as any number $\geqq 1$ for which

$$C \sum_{j=0}^{e_{n_0}} x^j/\Gamma(j/(l+1/n_0)+1) \geqq \beta(x) \text{ for } x \leqq d_{n_0+1}.$$

We set

$$b_j = C/\Gamma(j/(l+1/n_0)+1) \text{ for } j = 0, 1, \cdots, e_{n_0}.$$

Suppose that e_n and b_j have been defined for $j \leqq e_n$ with the property that $\sum_{j=0}^{e_n} b_j x^j \geqq \beta(x)$ for $0 \leqq x \leqq d_{n+1}$. Then we choose a_{n+1} as any integer $> e_n$ for which

$$\sum_{j=0}^{e_n} b_j x^j + \sum_{j=e_n+1}^{e_{n+1}} x^j/\Gamma(j/(l+1/(n+1))+1) \geqq \beta(x)$$

for $0 \leqq x \leqq d_{n+2}$. Then we define

$$b_j = 1/\Gamma(j/(l+1/(n+1))+1) \text{ for } j = e_n+1, \cdots, e_{n+1}.$$

It is readily verified that $B(x) = \sum b_j x^j$ has the desired properties.

We shall now give several examples of spaces $\mathcal{G}$. By use of Theorem 1, we shall thus be able to characterize the Fourier transforms of certain classes of functions. The simple direct method of characterizing the Fourier transforms of the spaces in Examples 1-6 (and in more general cases) is also carried out in Hörmander [1]. However, this method does not seem strong enough to obtain the topology of $\mathcal{D}'$ in Example 1.

Example 1. We choose for L_1 the class of all sequences $\{a_j\}$ for which $\sum a_j z^j$ defines an entire function, i.e. $a_j = O(k^{-j})$ for all $k > 0$. We take $C_1, C_2, \cdots, L_2, L_3, \cdots$ as the trivial class, that is, the class consisting of all finite sequences. A function $f \in \mathcal{S}$ will belong to $\mathcal{G}$ if and only if $\sum a_j X^j f^{(l)}$ converges in $\mathcal{S}$ for any $\{a_j\} \in L_1$, and any l. Such is clearly the case if f is of compact carrier, which means that f is in the space $\mathcal{D}$ of Schwartz (see Schwartz [1]). On the other hand, if $f \in \mathcal{G}$ then the product fg is bounded on R for any entire function g. It follows easily from this that f is of compact carrier. Thus, the elements of $\mathcal{G}$ and $\mathcal{D}$ are the same.

THEOREM 3. *With the choice C_j, L_j above, the topology of $\mathcal{G}$ is the same as that of $\mathcal{D}_F$* (see Ehrenpreis [3], [4]).

Proof. For any integer $s \geqq 0$, denote by $\mathcal{D}^s$ the space of all functions of compact carrier on R which are s times continuously differentiable; $\mathcal{D}^s$ is given the usual topology (see Ehrenpreis [3], Schwartz [1]). By definition, a set N in $\mathcal{D}_F$ is a neighborhood of zero in D_F if and only if, for some $s \geqq 0$, N is the intersection with $\mathcal{D}$ with a neighborhood of zero in $\mathcal{D}^s$. It is readily verified that the topology of D^s can be described as follows: A fundamental system of neighborhoods of zero in $\mathcal{D}^s$ consists of those set N for which we can find a continuous function h on R so that N consists of all $f \in \mathcal{D}^s$ which satisfy

$$\max_{x \in R,\, 0 \leqq r \leqq s} |h(x) f^{(r)}(x)| \leqq 1. \tag{2}$$

Now (see Lemma 1), given any continuous function k on R we can find an entire function[3] p on R such that, for all $x \in R$, $|k(x)| \leqq p(x)$. Thus, for a fundamental system of neighborhoods of zero in $\mathcal{D}^s$, it is sufficient to use only entire functions for h in (2). Theorem 1 results immediately.

It follows from this and the theorem of Paley and Wiener (see Schwartz [1], Ehrenpreis [1], [3], Paley and Wiener [1]) that $\mathfrak{S}$ consists of all entire functions of exponential type which are in $\mathcal{S}$. We shall now give an independent proof of this fact:

THEOREM 4. *With the choice of C_j, L_j as above, $\mathfrak{S}$ consists of all entire functions of exponential type which are in $\mathcal{S}$.*

Proof. First, let $F \in \hat{\mathfrak{S}}$; by Theorem 1, F is the Fourier transform of some $f \in \mathfrak{S}$. Since f is of compact carrier, it follows immediately that F is an entire function of exponential type in $\mathcal{S}$.

We shall, however, give proofs of this fact which is independent of the Fourier transform. This depends on the following proposition: Let F be any function which is indefinitely differentiable on R and for which $\sum a_j F^{(j)}(x)$ converges uniformly for x in any compact set of R whenever $\{a_j\} \in L_1$; then F is an entire function of exponential type. For, if we choose $\{a_j\} = \{1/j!\}$, then it follows that, given any finite interval $I \subset R$, we can find an $M > 0$ so that, for all $x \in I$, and all j,

$$|F^{(j)}(x)| \leqq Mj! \tag{3}$$

Relation (3) implies easily (see Mandelbrojt [2]) that F is analytic on R.

We claim that, for some $l > 0$, $F^{(j)}(0) = O(l^j)$. For, assume this is is not the case; then we can find an infinite sequence of increasing indices r_j so that, for all j,

$$|F^{(r_j)}(0)| \geqq j^{r_j}.$$

Define

$$b_k = \begin{cases} j^{-k} & \text{if } k = r_j \\ 0 & \text{otherwise.} \end{cases}$$

Then clearly $\{b_k\} \in L_1$, but

$$\sum b_k \,|\, F^{(k)}(0) = \infty.$$

This contradiction shows that $F^{(j)}(0) = O(l^j)$ for some $l > 0$. Since F is

[3] More precisely, we can find a function p on R which can be extended to an entire function. However, when speaking of analytic functions, we shall use the unprecise language of not distinguishing between an analytic function and its restriction to R, unless some possible confusion could result.

analytic on R, it follows immediately that F is an entire function of exponential type.

Conversely, let F be an entire function of exponential type $\leqq l$ in S. By a result of Phragmén and Lindelöf (see Titchmarsh [1], Schwartz [3]), $\exp(il\cdot)F$ is bounded in the upper half plane by $M=\max_{x\in R}|F(x)|$, where $\exp(a\cdot)$ is the function $x\to\exp(ax)$, and $\exp(-il\cdot)F$ is bounded in the lower half plane by M. For any $x\in R$, by Cauchy's formula,

$$(4)\qquad F'(x)=\frac{1}{2\pi i}\int_0^{2\pi}F(e^{i\theta})e^{-2i\theta}\,d\theta$$

$$=\frac{1}{2\pi i}\int_0^{\pi}F(e^{i\theta})e^{-2i\theta}\,d\theta+\frac{1}{2\pi i}\int_{\pi}^{2\pi}F(e^{i\theta})e^{-2i\theta}\,d\theta.$$

The first integral in (4), in modulus, does not exceed

$$\frac{1}{2\pi}\int_0^{\pi}M\,|\exp(-ile^{i\theta})|\,d\theta=(M/2\pi)\int_0^{\pi}\exp(l\sin\theta)\,d\theta.$$

Similarly,

$$\left|\frac{1}{2\pi i}\int_{\pi}^{2\pi}F(e^{i\theta})e^{-2i\theta}\,d\theta\right|\leqq(M/2\pi)\int_{-\pi}^{0}\exp(-l\sin\theta)\,d\theta.$$

Since, clearly,

$$\int_0^{\pi}\exp(l\sin\theta)=\int_{-\pi}^{0}\exp(-1\sin\theta)\,d\theta\leqq\pi e^{l},$$

we have, for any $x\in R$,

$$(5)\qquad |F'(x)|\leqq Me^{l}.$$

By iteration, for any n and any $x\in R$,

$$(6)\qquad |F^{(n)}(x)|\leqq Me^{ln}.$$

Hence, by the above-stated Phragmén-Lindelöf theorem, for any z with $|\mathfrak{I}(z)|\leqq 1$, and any n, ($\mathfrak{I}(z)$ denotes the imaginary part of z)

$$(7)\qquad |F^{(n)}(z)|\leqq Me^{l(n+1)}.$$

It results immediately from (7) that, for any sequence $\{a_n\}\in L_1$, $\sum a_nF^{(n)}(z)$ converges uniformly for $|\mathfrak{I}(z)|\leqq 1$. Now, for any $\{a_n\}\in L_1$, we have

$$(8)\qquad \sum_{n=0}^{r}a_nzF^{(n)}(z)=\sum_{n=0}^{r-1}a_n'F^{(n)}(z)+\sum_{n=0}^{r}a_n(FX)^{(n)}(z),$$

where $a_n'=(n+1)a_{n+1}$, as follows from the commutation relation between multiplication by X and $(d/dx)^j$:

$$(FX)^{(j)}-XF^{(j)}=jF^{(j-1)}$$

which is easily proved by induction. Now, for $\{a_n\} \in L_1$ $\{a_n'\}$ is again in L_1; moreover, FX is again an entire function of exponential type in $\mathcal{S}$. It follows from (8) and our previous remarks that $\sum a_n z F^{(n)}(z)$ converges uniformly for $|\mathcal{I}(z)| \leqq 1$. By iteration, for any j, $\sum a_n z^j F^{(n)}(z)$ converges uniformly in $|\mathcal{I}(z)| \leqq 1$. By Cauchy's formula, this implies that, for any j and any k, $\sum ((d^k/dx^k) a_n X^j F^{(n)})(x)$ converges uniformly in R. By the definition of the topology of $\mathcal{S}$ it follows that $\sum a_n F^{(n)}$ converges in $\mathcal{S}$. This completes of the proof of Theorem 4.

The topology of $\hat{\mathcal{G}} = \hat{\mathfrak{D}}_F$ is described in Ehrenpreis [3]. We give here first another expression for the topology of $\hat{\mathfrak{D}}_F$ and we show later that the two topologies are the same.

THEOREM 5. *Let a be any sequence such that $A(z) = \sum a_j z^j$ and $A^*(z) = \sum a^*_j z^j$ define entire functions of greater than exponential type; assume in addition that $i^j a_j > 0$ for all j. Let r be an integer and consider the set of $F \in \hat{\mathfrak{D}}_F$ which satisfy, for $s, k, p = 0, 1, 2, \cdots, r$*

$$\max_{\mathcal{I}(z)=y} |z^p (d^s/dz^s) F(z)| \leqq \begin{cases} A(iy) & \text{for } y \geqq 0 \\ A(-iy) & \text{for } y \leqq 0, \end{cases} \tag{9}$$

where $y = \mathcal{I}(z)$. Then the sets N form a fundamental system of neighborhoods of zero in $\mathfrak{D}_F$.

Proof. The fact that $A^*(z)$ is an entire function means that, for any l, $|a_j| \geqq l^j/j!$ for all but a finite number of l. This means that the sets N defined above have the property that, for any $F \in \hat{\mathfrak{D}}_F$, there is a $c > 0$ such that $cF \in N$. From this we deduce easily that the sets N define a locally convex topology on the set of functions of $\hat{\mathfrak{D}}_F$.

That each N is a neighborhood of zero in $\mathfrak{D}_F$ follows immediately from the fact that (see Lemma 2 above) conditions (9) are implied by

$$\max_{x \in R} |(d^p/dx^p) D^a X^k F(x)| \leqq 1/16(1+x^2) \tag{10}$$

for $p = 0, 1, 2$ and $k = 0, 1, 2, \cdots, r$.

To conclude the proof of Theorem 5 we must show that, for M any neighborhood of zero in $\hat{\mathfrak{D}}_F$, there exists an N as above with $N \subset M$. We may suppose that M is defined by an entire function $H(z) = \sum h_j z^j$ and an integer r so that M consists of all $F \in \hat{\mathfrak{D}}_F$ such that,

$$\max_{x \in R} |(d^s/dx^s) X^k D^h X^p F(x)| \leqq 1 \tag{11}$$

for $k, s, p = 0, 1, 2, \cdots, r$.

For each integer $l > 0$ we choose a positive number c_l so that $c_1 = 3$, $c_l < c_{l+1}$, and

$$h_l e^l / c_l^l \leqq 1/2^l.$$

Next we define the function g on the imaginary axis by $g(iy) = g(-iy) = e^l$ for $c_l + 1 \leqq y \leqq c_{l+1} + 1 - \epsilon$ (for some $\epsilon > 0$) and g is so defined as to be continuous and monotonic.

By Lemma 4 we can find an entire function H whose polar function H^* is entire such that $H(iy)$ has positive coefficients in its Taylor expansion and $H(iy) \leqq g(iy)$ for all y. Call N_0 the set of $F \in \hat{\mathfrak{D}}_F$ for which

$$(12) \qquad \sup_{\mathcal{G}(z)=y,\, y \geqq 2} |(d^s/dx^s) X^p F(x)| \leqq H(i\,|\,y\,|)/16(1+z^2)(2r)!$$

for $s, p = 0, 1, 2, \cdots, 2r$. By Cauchy's formula, for any $F \in N_0$, $F(z) = \sum f_j z^j$, we have

$$\begin{aligned} |\,h_j f_j\,| &= \left| \int_{ic_j-}^{ic_j+} z^{-(j+1)} F(z)\,dz \right| |\,h_j\,| \\ &\leqq |\,h_j\,|\, e^j / c_j{}^j r! \\ &\leqq 1/2^j r!. \end{aligned}$$

Thus, $(D^h F)(0) \leqq 1/(2r)!$. Similarly, for any z with $\mathcal{J}(z)| \leqq 1$, we have $|\,D^h F(z)\,| \leqq 1/(2r)!$. Applying the above to $X^p F$ in place of F $(p = 0, 1, 2, \cdots, 2r)$ we deduce that $|\,D^h X^p F(z)\,| \leqq 1/(2r)!$ for $p = 0, 1, 2, \cdots, 2r$, and for $|\,\mathcal{J}(z)\,| \leqq 1$.

For $k = 0, 1, 2, \cdots, r$ let $a = \{a_j{}^k\}$ be defined by

$$a_j{}^k = (j+1)(j+2)\cdots(j+k)a_{j+k}.$$

For each $k = 0, 1, 2, \cdots, r$ we determine a set N_k as above corresponding to the sequence a_k just as the set N_0 was determined corresponding to the sequence $a = a^0$. Then, by the above and induction on (8) it follows that

$$M \supset ((1/r!)N_0 \cap (1/r!)N_1 \cap \cdots \cap (1/r!)N_r).$$

This completes the proof of Theorem 5.

As an immediate consequence of Theorem 5, Lemma 4, and Cauchy's formula, we have

COROLLARY. *Let g be any continuous function on R such that, for every $c \geqq 0$, we can find an $\eta > 0$ such that $e^{c|x|} \leqq \eta g(x)$ for all $x \in R$. Let r be an integer and call N the set of $F \in \hat{\mathfrak{D}}_F$ which satisfy*

$$(12) \qquad \max_{I(z)=y} |z^p F(z)| \leqq f(y)$$

for all y and for $p=0,1,2,\cdots,r$. Then the sets N form a fundamental system of neighborhoods of zero in $\hat{\mathfrak{D}}_F$.

Remark. From the above Corollary it follows easily that the topology of $\hat{\mathfrak{D}}_F$ described above is the same as that described in Ehrenpreis [3].

Example 2. Let l be a positive number. L_1 consists of all sequences $\{a_n\}$ for which there is an $\epsilon > 0$ so that $\sum a_n z^n$ is analytic in the circle, center origin, radius $l+\epsilon$. $L_2, L_3, \cdots, C_1, C_2, \cdots$ are defined to be the trivial sets. It is easily seen that $\mathfrak{G}$ is just the space $\mathcal{D}_l$ (see Ehrenpreis [1], [3], Schwartz [1]) of indefinitely differentiable functions which vanish for $|x| \geqq l$. The topology of $\mathfrak{G}$ is the same as that of $\mathcal{D}_l$; this is a metrizable space in which a sequence $\{f_j\}$ converges to zero if and only if, for any k, $f_j^{(k)}(x) \to 0$ uniformly for $x \in R$.

Thus, $\hat{\mathfrak{G}}$ is the space $\hat{\mathfrak{D}}_l$ of all entire functions of exponential type $\leqq l$ which are in $\mathcal{S}$ (see Ehrenpreis [1], [3]). A sequence $\{F^j\}$ converges to zero in $\hat{\mathfrak{D}}_l$ if and only if, for any k, $(1+|z|^k)F^j(z) \to 0$ uniformly in $|\mathfrak{I}(z)| \leqq 1$. The method of proof of Theorem 4 is not quite strong enough to establish this characterization of $\hat{\mathfrak{G}}$ independently of the method of Ehrenpreis [3]. However, it was shown by Bernstein (see Schaeffer [1]) that the inequality (5) can be improved to

$$(5') \qquad |F(x)| \leqq Ml \quad \text{for all } x \in R$$

where, as in (5), F is an entire function of exponential type $\leqq l$ which is bounded by M on R. Using (5′) instead of (5) we can prove the above characterization of $\hat{\mathfrak{G}}$ by the method of proof of Theorem 4. The direct description of the topology of $\hat{\mathfrak{D}}_l$ can also be obtained by use of (a simplified form of) the method of proof of Theorem 5.

Example 2 provides us with an example in which the space $\mathfrak{G}$ is metrizable (although this situation does not seem to occur often).

Example 3. Let l be a positive number. L_1 consists of all sequences $\{a_n\}$ for which $\sum a_n z^n$ is analytic on the open circle, center origin, radius l. $L_2, L_3, \cdots, C_1, C_2, \cdots$ are the trivial sets.

The methods used to determine the spaces $\mathfrak{G}$, $\hat{\mathfrak{G}}$ are exactly the same as in Example 1. We can show that $\mathfrak{G}$ consists of all indefinitely differentiable functions which vanish outside of some compact subset of the interval $[-l < x < l]$. The space $\mathfrak{G}$ is topologically isomorphic to the space $\mathcal{D}_F$; the isomorphism can be given, e. g., by $f \in G \leftrightarrow h \in D_F$ where

$$f(x) = \begin{cases} h(\tan(\pi x/2)l)) & \text{for } |x| < l \\ 0 & \text{for } |x| \geqq l. \end{cases}$$

Example 4. Let l be a positive number. L_1 consists of all sequences $\{a_j\}$ for which $|\sum a_j z^j| = O(e^{l|z|})$, or, what is the same thing, $a_j = O(l^j/j!)$. $L_2, L_3, \cdots, C_1, C_2, \cdots$ are defined to consists of the finite sequences only.

It is readily verified that $\mathcal{G}$ is the space of all functions $f \in \mathcal{S}$ for which $\exp(l\cdot)f$ and $\exp(-l\cdot)f$ are again in $\mathcal{S}$. $\mathcal{G}$ is a metrizable space; a sequence $\{f_n\}$ converges to zero in $\mathcal{G}$ if and only if

$$\exp(l\cdot)f \to 0 \text{ in } \mathcal{S}, \qquad \exp(-l\cdot)f \to 0 \text{ in } \mathcal{S}.$$

$\hat{\mathcal{G}}$ consists of all functions F which are analytic in the strip $-l < \mathcal{I}(z) < l$ and continuous on the boundary with the additional properties

(a) Whenever $-l \leqq c \leqq l$, the function $x \to F(x+ic)$ lies in S.

(b) The set $\{x \to F(x+ic)\}_{-l \leqq c \leqq l}$ is bounded in S.

(By use of a generalization of the Phragmén-Lindelöf principle, it follows that conditions (a) and (b) are implied by much less stringent conditions on F; see Ehrenpreis [2].) A sequence $\{F_n\}$ converges to zero in $\hat{\mathcal{G}}$ if and only if, for any integer r, the sequences $x \to F_n(x \pm il)$ converge to zero in $\mathcal{S}$. This example as well as Example 5 below have also been considered by Schwartz [5] and Lions [1].

The proof of the above statements about the characterization and topology of $\hat{\mathcal{G}}$ can be proven in a simple manner by use of the Fourier transform. Thus, any $F \in \hat{\mathcal{G}}$ is the Fourier transform of an $f \in \mathcal{G}$ from which it follows immediately that F satisfies conditions (a) and (b) above. On the other hand, if F satisfies conditions (a) and (b), then, if f denotes the inverse Fourier transform of F, we have by Cauchy's theorem,

$$f(x) = e^{-lx} \int_{-\infty}^{\infty} F(t+il) e^{ixt}\, dt$$

$$f(x) = e^{lx} \int_{-\infty}^{\infty} F(t-il) e^{ix}\, dt.$$

It follows from the fact that the Fourier transform is a topological isomorphism of $\mathcal{S}$ onto $\mathcal{S}$ that $f \in \mathcal{G}$. By similar methods we can verify the above statement on the topology of $\hat{\mathcal{G}}$.

We can also give direct proofs of the characterization of $\hat{\mathcal{G}}$ and its topology without use of the Fourier transform.

Example 5 . Let l be a positive number. L_1 consists of all sequences

$\{a_j\}$ for which $A(z)=\sum a_j z^j$ is an entire function of exponential type $\leqq l$, that is, for every $\epsilon>0$, $A(z)=O(e^{(l+\epsilon)|z|})$. This is the same as saying that

$$\limsup(\log(j!\,|a_j|)/j)=\log l. \tag{13}$$

We write $\mathcal{K}_l$ for $\mathcal{G}$ and $\hat{\mathcal{K}}_l$ for $\hat{\mathcal{G}}$.

We have

THEOREM 6. *$f\in\mathcal{K}_l$ if and only if, for each r we can find an $\epsilon>0$ such that $f^{(r)}(x)=O(e^{-(l+\epsilon)|x|})$.*

COROLLARY. *A function F on R is in $\hat{\mathcal{K}}_l$ if and only if, for each integer n, we can find an $\epsilon_n>0$ so that Z^nF is bounded and analytic in the strip $|\mathfrak{I}(z)|\leqq l+\epsilon_n$.*

The above Corollary can be deduced easily from Theorem 6 by means of the Fourier transform; a direct proof can also be given.

Example 6. Let l be a positive number. L_1 consists of all sequences $\{a_j\}$ for which $A(z)=\sum a_j z^j$ is an entire function of order $\leqq l$, that is, for every $\epsilon>0$, $A(z)=O(\exp(|z|^{l+\epsilon}))$. This is the same as saying (see Titchmarsh [1], p. 253) that

$$\liminf(\log(1/|a_j|)/j\log j)=1/l. \tag{16}$$

We shall write $\mathfrak{A}_l$ for $\mathcal{G}$ and $\hat{\mathfrak{A}}_l$ for $\hat{\mathcal{G}}$.

THEOREM 7. *Let $f\in\mathcal{S}$; a necessary and sufficient condition that $f\in\mathfrak{A}_l$ is: For each k we can find an $\eta>0$ such that*

$$f^{(k)}(x)=O(\exp(-|x|^{l+\eta}).$$

Proof. The sufficiency of the condition is readily verified; we proceed to the necessity. Let $f\in\mathfrak{A}_l$ and assume that, for some k and for no $\eta>0$ is $f^{(k)}(x)=O(\exp(-|x|^{l-\eta})$. We suppose that $k=0$; the general case is handled similarly.

By our assumption, for any $n>0$ we can find a point $c_n\in R$ such that $f(c_n)\geqq\exp(-|c_n|^{l+1/n})$, and the $|c_n|\to\infty$. We shall construct a function H which is an entire function of order l and such that $H(c_n)\geqq\exp(|c_n|^{l+1/n})$. Thus, if $H(z)=\sum h_j z^j$, it is clear that f is not in the domain of X^h.

The construction of H proceeds along essentially the same lines as the proof of Lemma 1. We assume that all the c_n are positive and that $1<c_n<c_{n+1}$ for all n; the general case is easily reduced to this case or to the case where all c_n are negative and $1>c_n>c_{n+1}$ for all n, which is handled similarly. We set

$$H(z)=\sum_{j=0}^{\infty}\exp(c_n{}^{l-1/n})\,(z/c_n)^{e_n}, \tag{17}$$

where the integers e_n will be chosen so that H is an entire function of order l. Since $H(c_n) > \exp(c_n^{l+1/n})$, this will complete our proof. By (17) H will be of order $\leqq l$ if

$$\text{(18)} \qquad \log(c_n^{e_n}/\exp(c_n^{l+1/n}))/e_n \log e_n \geqq 1/(l+1/n) - \epsilon_n \text{ for all } n,$$

where $\epsilon_n \to 0$. The left side of (18) is

$$[e_n \log c_n - c_n^{l+1/n}]/e_n \log e_n = \log c/\log e_n - c_n^{l+1/n}/e_n \log e_n.$$

We choose $e_n = [c_n^{l+1/n}]$ where, for $x \in R$, $[x]$ is the greatest integer $\leqq x$. We may clearly assume that the c_n are so chosen that $e_n < e_{n+1}$ for all n. Then the left side of (18) is $\geqq 1/(l+1/n) - \epsilon_n$, where we may choose $\epsilon_n = e_n + 1/e_n \log e_n$ so that $\epsilon_n \to 0$. This completes the construction of H and so completes the proof of Theorem 7.

Theorem 7 shows that the space in Example 6 is the same as a space considered by Gelfand and Silov [1].

We can also prove, either directly or by means of Fourier transform,

THEOREM 8. *Let $l \geqq 1$ and let F be an entire function in $\mathcal{S}$. A necessary and sufficient condition that $F \in \hat{\mathfrak{A}}_l$ is: For any integer $n \geqq 0$ we can find an $\eta' > 0$ so that*

$$\text{(19)} \qquad \sup_{\mathcal{I}(z)=y} |z^n F(z)| = O(\exp(|y|^{l'-\eta'})),$$

where l' is the conjugate exponent of l, i.e. $1/l + 1/l' = 1$.

THEOREM 9. *Let h be any continuous positive function on R such that, for every $\epsilon > 0$, $\exp(-|x|^{l+\epsilon}) = O(h(x))$; let m be an integer. Call N the set of $f \in A_l$ which satisfy, for all $x \in R$,*

$$\text{(22)} \qquad |f^{(k)}(x)| \leqq h(x) \text{ for } k = 0, 1, 2, \cdots, m.$$

Then these sets N form a fundamental system of neighborhoods of zero in A_l.

THEOREM 10. *Let $l \geqq 1$; let g be any continuous function on R such that, for every $\epsilon > 0$, $\exp(|x|^{l'-\epsilon}) = O(g(x))$; let m be a positive integer. Call M the set of $F \in \hat{\mathfrak{A}}_l$ such that*

$$\text{(24)} \qquad \sup_{\mathcal{I}(z)=y} |z^k F(z)| \leqq g(y) \text{ for } k = 0, 1, \cdots, m.$$

Then the sets M form a fundamental system of neighborhoods of zero in $\hat{\mathfrak{A}}_l$.

Example 7, non quasi-analytic classes. Up to now, we considered spaces $\mathfrak{G}$ and $\hat{\mathfrak{G}}$ for which only one of the C_i, L_i was non-trivial. For the next example, we choose L_1 as consisting of all sequences $\{a_j\}$ for which $\sum a_j z^j$ is an entire function. C_1 consists of all sequences $\{b_j\}$ such that $\sum b_j z^j$ is an

entire function of order l, where $l < 1$ is fixed. C_j and L_j for $j > 1$ are defined to be trivial sets. We write $\mathfrak{J}_l$ for $\mathfrak{G}$ and $\hat{\mathfrak{J}}_l$ for $\hat{\mathfrak{G}}$.

The space $\mathfrak{J}_l$ consists of those functions f of compact carrier which satisfy

$$f^{(k)}(x) = O(k^{k/l'}) \text{ uniformly in } x \tag{27}$$

for some $l' > l$. This follows readily from equation (16). Thus, if $l \geqq 1$, f would have to be analytic, so $\mathfrak{J}_l$ would consist of $\{0\}$ only. If $l < 1$, it is well-known (see Paley and Wiener [1], Mandelbrojt [2]) that $\mathfrak{J}_l$ is non-empty. We shall see later that, in fact, $\mathfrak{J}_l$ is dense in $\mathfrak{D}$.

For the use of the spaces $\mathfrak{J}_l$ in partial differential equations, see e.g. Ehrenpreis [7], [10], [11], [12], Hörmander [1], [3], Friedman [1].

Using Theorem 4 and methods similar to the above, we can deduce

THEOREM 11. *$\hat{\mathfrak{J}}_l$ consists of all entire functions F of exponential type which satisfy*

$$F(x) = O(\exp(-|x|^{l+\eta})) \tag{28}$$

for some $\eta > 0$.

We can now prove

THEOREM 12. *For any $l < 1$, $\mathfrak{J}_l$ is dense in $\mathfrak{D}$.*

Proof. It follows from the above Theorem 11 that $\mathfrak{J}_l$ is an (algebraic) ideal in $\mathfrak{D}$ under convolution. Moreover, since $\mathfrak{J}_l$ is non empty, we can find a function $f \in \mathfrak{J}_l$ which is not identically zero. Then if c is any zero of F with order r, it follows from Theorem 11 that $F(z)/(z-c)^r$ is again in $\mathfrak{J}_l$. Thus, the (algebraic) ideal $\hat{\mathfrak{J}}_l$ has no common zeros. It follows from the fundamental theorem of mean periodic functions (see Schwartz [4], Ehrenpreis [5]) that $\mathfrak{J}_l$ is dense in $\mathfrak{D}$, which is the desired result.

Remark. By a similar method we could show that $\mathfrak{J}_l$ is dense in $\mathfrak{J}_{l'}$ whenever $l > l'$.

We consider first the topology of $\mathfrak{J}_l$:

THEOREM 13. *Let γ be any continuous positive function on C such that, for any ϵ, k, we have $(z = x + iy)$*

$$\exp(-|x|^{l+\epsilon} + k|y|) = O(\gamma(x,y)), \tag{29}$$

and γ is the product of a function of x by a function of y. Let N be the set of $F \in \hat{\mathfrak{J}}_l$ which satisfy

$$|F(z)| \leqq \gamma(z) \text{ for all } z \in C.$$

Then these sets N form a fundamental system of neighborhoods of zero in $\hat{\mathfrak{J}}_l$.

Proof. Let us note the following: A set $M \subset \hat{\mathfrak{J}}_l$ is a neighborhood of zero if and only if we can find a neighborhood of zero P in $\mathfrak{D}_F$ and entire functions $B_1, B_2, \cdots, B_r$ of order l such that M consists of all $F \in \hat{J}_l$ for which $B_j F \in P$ for $j = 1, 2, \cdots, r$. This follows readily from the definition of the topologies of $\hat{D}_F$ and J_l by means of infinite derivatives.

Now, by Theorem 5, there are a continuous function A on R and an integer s so that P consists of all $G \in D_F$ which satisfy $(z = x + iy)$

$$| z^p G(z) | \leqq A(y)$$

for $p = 1, 2, \cdots, s$, and for all $z \in C$; A is a positive function with the property that $\exp(k\,|\,y\,|) = O(A(y))$ for all k. Thus $F \in \hat{\mathfrak{J}}_l$ is in M if and only if, for $j = 1, 2, \cdots, r$, $p = 1, 2, \cdots, s$, we have

$$(30) \qquad | z^p B_j(z) F(z) | \leqq A(y)$$

for all $z \in C$.

Let us set

$$\alpha(w) = \max_{j=1,2,\cdots,r,\, p=1,2,\cdots,s,\, |z|=2w} | z^p B_j(z) |,$$

so α is of order l, that is, $\alpha(w) = O(\exp(|\,w\,|^{l+\epsilon}))$ for every $\epsilon > 0$. We define

$$(31) \qquad \gamma(z) = A(y)/[1 + \alpha(|\,y\,|)][1 + \alpha(|\,x\,|)].$$

Then it is readily verified that γ satisfies the hypotheses of Theorem 13.

If $F \in \hat{\mathfrak{J}}_l$ satisfies $|F(z)| \leqq \gamma(z)$ for all z, then we have, for any j, p,

$$| z^p B_j(z) F(z) | \leqq | z^p B_j(z) |\, A(y)/[1 + \alpha(|\,y\,|)][1 + \alpha(|\,x\,|)].$$

Now, either $|\,y\,|$ or $|\,x\,|$ is $\geqq \frac{1}{2}|\,z\,|$ so that

$$| z^p B_j(z) |/[1 + \alpha(|\,y\,|)][1 + \alpha(|\,x\,|)] \leqq 1.$$

Thus the condition $|F(z)| \leqq \gamma(z)$ implies

$$| z^p B_j(z) F(z) | \leqq A(y)$$

for $p = 1, 2, \cdots, s$, $j = 1, 2, \cdots, r$ and all y. This means that $F \in M$.

We have shown that every neighborhood of zero in $\hat{\mathfrak{J}}_l$ contains a set N as described in the statement of our theorem. It remains to show that these sets N are neighborhoods of zero in J_l. To this end, let γ be any function satisfying (31). We set

$$(32) \qquad \beta(x) = \gamma(x, 0).$$

Then it follows from (31) that, for any $\epsilon > 0$,

$$(33) \qquad \exp(-|\,x\,|^{l+\epsilon}) = O(\beta(x)).$$

Next, we choose a fixed $\eta > 0$ so that $l + \eta < 1$. We set

$$A(2y) = \gamma(0, y)\exp(-|3y|). \tag{34}$$

It is clear that, for any k,

$$\exp(k|y|) = O(A(y)).$$

We may assume, without any loss in generality, that β is even and monotonically decreasing and that A is even and monotonically increasing.

Next (see (33) and Lemma 6 above), we choose an entire function B of order l such that $B(z+1)$ has positive Taylor coefficients at zero, $B(-1) \geqq 1$, and $B(x) \geqq 1/\beta(x+1)$, for $x \geqq -1$, and $|B(x)/B(x-1)|$ is bounded for $x \geqq 0$. Let M be the set of $F \in \hat{\mathfrak{H}}_l$ which satisfy

$$|F(z)B(z)| \leqq A(y), \qquad |F(z)B(-z)| \leqq A(y),$$

for all $z = x + iy$; by what we have said above, M is a neighborhood of zero in $\hat{\mathfrak{H}}_l$. We claim that, for a suitable choice of $c > 0$, $cM \subset N$.

For this purpose, we have to note that the function B could be modified slightly so that we can assume that B is large in some angular sector containing the positive real axis. For, we can easily extend Lemma 13 below so as to mawe an inequality like (70):

$$\alpha|\mathcal{R}\, Q(z)| \leqq |\mathcal{R}\exp(z^r)| \leqq \beta|\mathcal{R}\, Q(2z)| \tag{70'}$$

hold in a sufficiently small angular sector containing the positive real axis. ($\mathcal{R}$ denotes the real part.) Then the proof of Lemma 6 can be modified to show (using the minimum modulus theorem 5 of [5] to handle small values of x) that we can assume B has the property stated in:

LEMMA 7. *We can find a constant d so that, given any y_0 we can find a y' lying between y_0 and $2y_0$ such that for any $x \geqq 0$,*

$$B(x+iy') \geqq d\exp(-|y'|)/\beta(x). \tag{35}$$

Moreover

$$B(x+iy') \geqq d\exp(-|y'|)|B(x-1)|. \tag{36}$$

Thus, any $F \in M$ satisfies, for $x \geqq 0$,

$$\begin{aligned} |F(x+iy')| &\leqq A(y')/|B(x+iy')| \\ &\leqq dA(y')\beta(x)\exp(|y'|) \\ &\leqq dA(2y_0)\beta(x)\exp(|3y_0|) \\ &= d\gamma(x, y_0). \end{aligned} \tag{37}$$

Now, inequality (37) is not good enough because it is only proven for some y' lying between y_0 and $2y_0$. In order to complete the proof of our theorem, we consider $B(z-iy_0)F(z)$ instead of $F(z)$. We have, for all $x \geqq 0$, (see Lemma 8 below) by Lemma 7,

$$(38)\quad \begin{aligned} |B(x+iy'-iy_0)F(x+iy')| &\leqq B(x)\exp(|y'-y_0|)|F(x+iy')| \\ &\leqq B(x)\exp(|y_0|)|F(x+iy')| \\ &\leqq (1/d)(B(x)/|B(x-1)|)\exp(|y_0|)A(2y_0)\exp(|2y_0|). \end{aligned}$$

By Lemma 8 below, $|B(x)/B(x-1)| \leqq e$ for all $x \geqq 0$. Thus,

$$(39)\quad |B(x+iy'-iy_0)F(x+iy')| \leqq (e/d)\exp(|3y_0|)A(2y_0)$$

for all $x \geqq 0$ and similarly for all $x \leqq 0$. Similarly, we can find a y'' lying between $-y_0$ and $-2y_0$ for which an inequality similar to (39) holds. Thus, by the maximum modulus theorem applied to the strip lying between y' and y'', we have

$$(40)\quad |B(|x|)F(x+iy_0)| \leqq (e/d)\exp(|3y_0|)A(2y_0),$$

or

$$\begin{aligned} |F(x+iy_0)| &\leqq (e/d)\exp(|3y_0|)A(2y_0)/B(|x|) \\ &\leqq (e/d)\exp(|3y_0|)A(2y_0)\beta(x) \\ &\leqq (e/d)\gamma(x,y_0). \end{aligned}$$

Thus, if we choose $c=d/e$, we have $cF \in N$. This proves that $cM \subset N$ which concludes the proof of Theorem 13.

We have used in the proof of Theorem 13

LEMMA 8. *Let B, η be as above; then we have*

$$|B(x+y)| \leqq B(x)\exp(|y|)$$

for all $x \geqq -1$ and all y (real or complex).

Proof. We write $B(x_0)=\sum b_j(x_0+1)^j$. Then if $x_0 \geqq -1$, the Taylor coefficients of B at x_0 are

$$(41)\quad b_k(x_0)=(1/k!)\sum_{j=0}^{\infty} j(j-1)\cdots(j-k)(x_0+1)^{j-k}b_j.$$

By our construction of B (see Lemma 6), we know that, for all j, we have $jm_j \leqq b_{j-1}$, so that $j(j-1)\cdots(j-k)b_j \leqq b_{j-k}$. This gives, by (41),

$$b_k(x_0) \leqq (1/k!)\sum_{j=0}^{\infty} b_{j-k}(x_0+1)^{j-k}=B(x_0)$$

because all the b_t are positive. Thus, for $x \geqq -1$,

$$
\begin{aligned}
(42) \qquad | B(x+y) | &\leqq B(x+|y|) \\
&= \sum b_k(x) | y |^k \\
&\leqq B(x) \sum | y |^k / k! \\
&= e^{|y|} B(x).
\end{aligned}
$$

This is the desired result.

The topology of $\mathfrak{J}_l$ is very closely related to that of $\mathfrak{D}_F$. In fact, we have

THEOREM 14. *The topology of $\mathfrak{J}_l$ can be described as follows:*

(1) *Let $a(z) = \sum a_j z^j$ be an entire function of order l, and let b be an entire function. Let N be the set of $f \in \mathfrak{J}_l$ for which*

$$
(43) \qquad \max_{x \in R} | b(x) | \sum | a_j f^{(j)}(x) | \leqq 1.
$$

Then the sets N form a fundamental system of neighborhoods of zero in $\mathfrak{J}_l$.

(2) *Let $c = \{c_j\}$ be any sequence of positive numbers such that, for any $l' > l$, we have*

$$
(44) \qquad j^{j/l'} = O(c_j).
$$

Let e be an entire function, and let M be the set of $f \in \mathfrak{J}_l$ which satisfy, for all $x \in R$,

$$
(45) \qquad | f^{(j)}(x) | \leqq c_j | e(x) |.
$$

Then these sets M constitute a fundamental systems of neighborhoods of zero in $\mathfrak{J}_l$.

Proof. (1) It is easily seen from the definitions that every neighborhood of zero in $\mathfrak{J}_l$ is contained in some N. Thus, we have to show that the sets N are neighborhoods of zero. This is not at all obvious because the topology of $\mathfrak{J}_l$ is defined in terms of sums whereas the sets N are described in terms of absolute values.

To prove Theorem 14 we use our previous Theorem 13 on the characterization of the Fourier transform $\hat{\mathfrak{J}}_l$. We want to produce a neighborhhod of zero N' in $\hat{\mathfrak{J}}_l$ such that for any $F \in N'$, we have $f \in N$.

For $j = 0, 1, 2, \cdots$, let $e_j = \max_{j' \geqq j} | a_{j'} |$, so $\{e_j\}$ is montonically decreasing and $\sum e_j z^j$ is an entire function e of order l. We set $\gamma_1(x) = [1 + e(|x|)]^{-1}$.

We define $\gamma_2(y)$ as follows: $\gamma_2(0)=1$. For each $j>0$, let $j'=j'(j)>0$ be so chosen that $\exp(jj')\geqq \max_{|x|\leqq j} b(x)$; then set $\gamma_2(\pm j')=\exp(jj')$. The definition of γ_2 is completed by requiring that γ_2 be continuous and monotonic.

Set

$$\gamma(z)=\gamma_1(x)\gamma_2(y)(1+x^2)^{-1}. \tag{46}$$

Let N' be the set of $F\in \hat{\mathfrak{J}}_l$ for which $|F(z)|\leqq\gamma(z)$ for all $z\in C$. By Theorem 13, N' is a neighborhood of zero in $\hat{\mathfrak{J}}_l$. We shall produce a $c>0$ so that $F\in N'$ implies $cf\in N$.

Let $F\in N'$. Then for $t\geqq 0$,

$$\begin{aligned}
\sum|a_j f^{(j)}(t)| &= \sum|a_j\int x^j F(x)\exp(itx)\,dx| \\
&= \sum|a_j\int_{\mathcal{J}(z)=j'([t]+1)} z^j F(z)\exp(itz)\,dz| \\
&\leqq \sum|a_j|\int_{\mathcal{J}(z)=j'([t]+1)}|z|^j\,|F(z)|\exp(-tj'([t]+1))dz \\
&\leqq \exp(-tj'([t]+1))\int_{\mathcal{J}(z)=j'([t]+1)}\sum|a_j|\,|z|^j\,|F(z)|\,dz \\
&\leqq \exp(-tj'([t]+1))\int_{\mathcal{J}(z)=j'([t]+1)} e(|z|)\gamma(z)dz \\
&\leqq \exp(-tj'([t]+1))\int e(|x|+j'([t]+1))\gamma_1(x)\gamma_2(j'([t]+1))(1+x^2)^{-1}\,dx \\
&\leqq \exp(-(t-1)j'([t]+1))\gamma_2(j'[t]+1)\int e(|x|)\gamma_1(x)(1+x^2)^{-1}\,dx
\end{aligned}$$

because we can assume, by modifying e if necessary that (see Lemma 8) $e(|x|+|\alpha|)\leqq e(|x|)\exp(|\alpha|)$, where we have written $[t]$ for the greatest integer $\leqq t$.

Now, we have, by definition,

$$\gamma_2(j'[t]+1)=\exp[([t]-2)j'([t]+1)]$$

so that

$$\begin{aligned}
\exp[-(t-1)j'([t]+1)]\gamma_2(j'[t+1]) &\leqq \exp(-j'([t]+1)) \\
&\leqq [\max_{|s|\leqq[t]+1}|b(s)|]^{-1} \\
&\leqq |b(t)|^{-1}.
\end{aligned}$$

Moreover, we have $\int e(|x|)\gamma_1(x)(1+x^2)^{-1}\leqq 1$. Thus,

$$\sum|a_j f^{(j)}(t)|\leqq|b(t)|^{-1} \tag{47}$$

if $t > 1$. A similar argument applies if $t < -1$. Moreover, for any t we have

$$\begin{aligned}\sum |a_j f^{(j)}(t)| = \sum |a_j \int x^j F(x) \exp(itx)\,dx| &\leqq \int e(|x|)\,|F(x)|\,dx \\ &\leqq \int e(|x|)\gamma_1(x)(1+x^2)^{-1} \\ &\leqq 1.\end{aligned}$$

It follows that $[\max_{|t|\leqq 2} |b(t)|]^{-1} f \in N$, which is the desired result.

(2) The equivalence of (1) and (2) is readily verified.

Remark. It has been necessary to use the Fourier transform to prove Theorem 14. A direct proof of this theorem is undoubtedly very difficult to obtain.

Besides being useful in the study of differential equations and elliptic operators (see Ehrenpreis [7] and [10]), the spaces $\mathfrak{J}_l$ exhibit a remarkable property as topological vector spaces: Let us denote, for any $t > 0$, by $\mathfrak{J}_l^t$ the space for all $f \in \mathfrak{J}_l$ such that $f(x) = 0$ if $|x| > t$. We give $\mathfrak{J}_l^t$ the topology induced from $\mathfrak{J}_l$. We call λ the topology of the inductive limit of the spaces $\mathfrak{J}_l^t$ for t integral, so λ is another topology on $\mathfrak{J}_l$ (see Dieudonné and Schwartz [1]. Strictly speaking, only the inductive limit of Frechet spaces is defined in Dieudonné and Schwartz [1], but the definitions do not require the Frechet property.) We shall show that the topology λ is the same as that of $\mathfrak{J}_l$. Note that the analogous property does not hold for the space $\mathfrak{D}$, namely, the topologices of $\mathfrak{D}$ and $\mathfrak{D}_F$ are different.

First we need

LEMMA 9. *For any $l < 1$, we can find a sequence of non-negative functions $h_j \in \mathfrak{J}_l$ such that*

a) carrier $h_j \subset [j'-1 \leqq x \leqq j'+1]$ *for some j', and for at most 3 values of j does* carrier h_j *intersect* $[j'-1 \leqq x \leqq j'+1]$.

b) *For any $x \in R$, $\sum h_j(x) = 1$.*

Proof. Let

$$f_p(x) = \begin{cases} \exp(-x^{-p}) & \text{if } x > 0 \\ 0 & \text{if } x \leqq 0. \end{cases} \tag{48}$$

We want to obtain bounds on the derivatives of f_p. (The f_p are clearly indefinitely differentiable.) First we compute the maximum of $x^{-r} f_p(x)$. Differentiating we obtain, for $x > 0$,

$$\begin{gathered} -rx^{-r-1}\exp(-x^{-p}) + px^{-r-p-1}\exp(-x^{-p}) = 0 \\ p - rx^p = 0, \qquad x = (p/r)^{1/p}. \end{gathered}$$

Thus the maximum of $x^r f_p(x)$ is $(r/p)^{r/p}\exp(-r/p)$.

Now, the k-th derivative of f_p is a sum of terms of the form $e_j x^{-j} f_p(x)$, where $j = l(p+1) + (k-l)$ for some $l \leqq k$, and then

$$e_j \leqq [l(p+1) + (k-l)]^{k-l}(p+1)^l.$$

Thus, using the above, we find that

$$\begin{aligned} \max e_j f_p(x) &\leqq (p+1)^l (lp+k)/p + kl \\ &\leqq (p+1)^l (lp+k)^{k(1+1/p)} \\ &\leqq (p+1)^l (kp+k)^{k(1+1/p)} \\ &\leqq (p+1)^{3k} k^{k(1+1/p)} \end{aligned}$$

because $l \leqq k$. Since the number of terms $e_j f_j(x)$ is 2^k, we see that

$$\max_{x \in R} | f_p^{(k)}(x) | \leqq 2^k (p+1)^{3k} k^{k(1+1/p)}. \tag{49}$$

Now we use (49); it follows that if $\sum a_j z^j$ is an entire function of order $\leqq l$, then $\sum a_j f_p^{(j)}(x)$ will converge uniformly for $x \in R$ if $p > l(1-l)$.

By forming products, translates, and integrals of the f_p, we can easily construct functions satisfying the hypotheses of Lemma 9.

Now we wish to describe the topology λ explicitly:

PROPOSITION 5. *Let $\{a^k(z)\} = \{\sum a_j^k z^j\}$ be a sequence of entire functions of order $\leqq l$. Let N be the set of $f \in \mathfrak{J}_l$ which satisfy*

$$\max_{k-1 \leqq |x| \leqq k+1} \sum | a_j^k f^{(j)}(x) | \leqq 1. \tag{50}$$

Then these sets N form a fundamental system of neighborhoods of zero for λ.

Proof. It follows immediately from Theorem 14 that $N \cap \mathfrak{J}_l^r$ is a neighborhood of zero in $\mathfrak{J}_l^r$ for all r; since N is convex, N is a neighborhood of zero for λ. Conversely, let M be a convex neighborhood of zero in $\mathfrak{J}_l^r$. We can assume that we can find an entire function of order $\leqq l$, $b^r(z) = \sum b_j^r z^j$, so that M^r contains the set of $f \in \mathfrak{J}_l^r$ with

$$\max_{x \in R} | \sum b_j^r f^{(j)}(x) | \leqq 1.$$

Let us note the following: For any $f \in \mathfrak{J}_l$, and any k, $f_k = h_k f$ (where the h_k are as in Lemma 9) is again in $\mathfrak{J}_l$. Moreover, we can write, for any $x \in R$,

$$\begin{aligned} \sum b_j^r f_k^{(j)}(x) &= \sum b_j^r (f h_k)^j (x) \\ &= \sum b_j^{r,k}(x) f^{(j)}(x), \end{aligned}$$

where for each x we have $\sum b_j^{r,k}(x) z^j$ is an entire function of order $\leqq l$ and,

moreover, if $c_j^{r,k} = \max_{x \in R} | b_j^{r,k}(x) |$, then $\sum c_j^{r,k} z^j$ is an entire function of order $\leqq l$. For each r only a finite number of k have the property that the carrier of k meets $[-r-1 \leqq x \leqq r+1]$; we define c_j^r as the maximum of $c_j^{r,k}$ over these k, so $\sum . c_j^r z^j$ is an entire function of order $\leqq l$.

We define N as the set of $f \in \mathfrak{J}_l$ for which

$$\sup_{r-1 \leqq |x| \leqq r+1} \sum | c_j^r f^{(j)}(x) | \leqq 3^{-r-3}. \tag{51}$$

We claim that $N \subset M$. For any $f \in N$ write $f = \sum f_k$, where $f_k = h_k f$. Let r be so chosen that *carrier* $h_k \subset [| x | \leqq r+1]$; by our construction there are at most $3r$ values of k corresponding to any value of r. Next we have, if $| x | \leqq r+1$,

$$\begin{aligned} | \sum b_j^r f_k^{(j)}(x) | &\leqq \sum | b_j^r f_k^{(j)}(x) | \\ &\leqq \sum | c_j^r f^j(x) | \\ &\leqq 3^{-r-3}. \end{aligned}$$

Thus, $3^{r+3} f_k \in M^r \subset M$. Since M is convex, we have $f = \sum_{(\text{finite})} f_k \in M$. Thus $N \subset M$ which is the desired result.

THEOREM 15. *The topology λ is the same as that of $\mathfrak{J}_l$.*

Proof. Since the topologies induced by $\mathfrak{J}_l$ and λ on $\mathfrak{J}_l^r$ are, for any r, just the topology of J_l^r, it follows from the definition of an inductive limit (see Dieudonné and Schwartz [1]) that the topology λ is stronger than that of $\mathfrak{J}_l$. (This also follows immediately from Proposition 5.)

Let N be a neighborhood of zero for λ; by Proposition 5 we can find entire functions $a^k(z) = \sum a_j^k z^j$ of order $\leqq l$ so that N contains the set of $f \in \mathfrak{J}_l$ for which

$$\max_{k-1 \leqq |x| \leqq k+1} \sum | a_j^k f^{(j)}(x) | \leqq 1.$$

We define the sequence $\{b_n\}$ as follows: $b_0 = 1$, $b_n = \exp[-(l - l^2) \log n]$ for $n = 1, 2, \cdots, n_1$, where $n_1 \geqq 1$ is so chosen that $| a_j^k | \leqq \exp(-(l - l^2) \log j)$ whenever $k \leqq 2$ and $j \geqq n_1$. Suppose that b_n has been defined for $n \leqq n_p$, where $p \geqq 1$, and $n_p \geqq p$. Then we set

$$b_n = \exp(-(l - l^{p+2})) \text{ for } n = n_p + 1, n_p + 2, \cdots, n_{p+1},$$

where $n_{p+1} > n_p$ is so chosen that $| a_j^k | \leqq \exp[-(l - l^{p+3})]$ whenever $k \leqq p+2$ and $j \geqq n_{p+1}$. It is clear that the numbers n_p can be found and, moreover, that $\sum b_j z^j$ is an entire function of order l.

Now, we have, for any k, $| a_j^k | \leqq b_j$ for all but a finite number of j.

Thus, we can find a constant $c_k > 0$ with $c_k \mid a_j^k \mid \leqq b_j$ for all j. Call M the set of $f \in \mathfrak{J}_l$ which satisfy, for all k,

$$\max_{k-1 \leqq |x| \leqq k+1} \sum | b_j f^{(j)}(x) | \leqq c_k. \tag{52}$$

By Theorem 14, M is a neighborhood of zero in $\mathfrak{J}_l$; we claim that $M \subset N$.

Let $f \in M$, then if $k-1 < |x| \leqq k+1$,

$$\begin{aligned} \sum | a_j^k f^{(j)}(x) | &\leqq (1/c_k) \sum | b_j f^{(j)}(x) | \\ &\leqq 1 \end{aligned}$$

because of (52). Thus $f \in N$, which concludes the proof of Theorem 15.

Example 7′. We choose C_1 as the set of all sequences $\{a_n\}$ for which $a_n = O(\epsilon^n/\Gamma(rn))$ for some $\epsilon > 0$. L_1 consists of all sequences $\{b_n\}$ such that $\sum b_n z^n$ is an entire function. We define C_j and L_j to be trivial for $j > 1$. We denote the space $\mathfrak{G}$ obtained by ${}_r\mathfrak{D}$. The spaces ${}_r\mathfrak{D}$ play an important role in the study of elliptic operators and Cauchy's problem in partial differential equation (see Ehrenpreis [7], [10]).

By using methods similar (and, in fact, simpler) than those employed in the proof of Theorems 11 and 13, we can deduce

THEOREM 11′. *${}_r\hat{\mathfrak{D}}$ consists of all functions F of exponential type which satisfy for some $A > 0$,*

$$| F(x) | = O(\exp(-A \, | x |^{r'})), \tag{28′}$$

where $r' = 1/r$.

THEOREM 13′. *Let γ be any continuous positive function on C such that for all $A > 0$ and some k we have $(z = x + iy)$*

$$\exp(-A \, | x |^{r'} + k \, | y |) = O(\gamma(x, y)) \tag{29′}$$

and γ is the product of a function of x by a function of y. Let N be the set of $F \in {}_r\mathfrak{D}$ which satisfy

$$| F(z) | \leqq \gamma(z) \text{ for all } z \in C.$$

Then these sets N form a fundamental system of neighborhoods of zero in ${}_r\hat{\mathfrak{D}}'$.

II. Infinite derivatives for $\mathcal{E}$. By $\mathcal{E}$ we denote the space of all indefinitely differentiable functions on R with the Schwartz topology (see Schwartz [1]): $\mathcal{E}$ is metrizeable; a sequence $\{f^j\}$ converges to zero in $\mathcal{E}$ if and only if the f^j and all their derivatives converge to zero uniformly on every compact set of R.

Now, the space $\mathcal{S}$, which played a fundamental role in Chapter I, was defined by both regularity conditions and growth conditions at infinity. In contrast to this, the space $\mathcal{E}$ is defined solely in terms of regularity conditions. Thus, only the operator d/dx will be used to define the spaces of functions which we consider here, while only the operator X will be needed to define the space of Fourier transforms.

Let $a = \{a_j\}$ be a sequence of complex numbers. We say that $f \in \mathcal{E}$ is *in the domain of* D^a *(for the space* $\mathcal{E}$*)* if $\sum a_j f^{(j)}$ converges in the space $\mathcal{E}$ and if, moreover, for each $k > 0$ we have $\sum | a_j f^{(j+k)}(x) |$ converges uniformly for x in any compact set of R; when no confusion can arise, we shall merely state that f is in the domain of D^a, and we set $D^a f = \sum a_j f^{(j)}$.

Let A be a class of sequences $\{a_j\}$. We define the space $\mathcal{P}$ to consist of all $f \in \mathcal{E}$ which are in the domain of D^a for all $a \in A$. The topology of $\mathcal{P}$ is defined by the semi-norms

$$\sup_{x \in K} \sum | a_j f^{(j+k)}(x) | \tag{53}$$

for K any compact set in R and $\{a_j\}$ any sequence in A and any integer $k \geqq 0$

Remark. $\mathcal{P}$ may not be Hausdorf even if A is non-empty. E.g. A consists of the single sequence: $a_0 = 0$, $a_1 = 1$, $a_j = 0$ for $j > 0$. Then $f(x) = x$ is not separated from 0. The results of the theory of mean-periodic functions (see Schwartz [4], Ehrenpreis [5]) seem to indicate that if all the functions $\sum a_j z^j = a(z)$ for $\{a_j\} \in A$ are entire functions, then $\mathcal{P}$ will be Hausdorf if, for any $\{a_j\} \in A$, the sequence $\{a_j'\}$ also lies in A where $\{a_j'\}$ is obtained from $\{a_j\}$ by some small deformation. $\mathcal{P}$ will not be Hausdorf if the $a(z)$ have a common zero z_0, for then $\exp(z_0 x)$ will satisfy $D^a \exp(z_0 x) = 0$ for all $a \in A$, and thus cannot be separated from 0.

Problem. Can we replace the semi-norms in (53) by the semi-norms

$$\sup_{x \in K} | \sum a_j f^{(j+k)}(x) | = \sup_{x \in K} | D^a f^{(k)}(x) | \, ? \tag{54}$$

This problem seems to be very difficult. In particular, I do not know whether or not the semi-norms (54) lead to a complete space.

The set A will be called *admissible* if every finite sequence belongs to A. It is readily verified that the corresponding space $\mathcal{P}$ is always Hausdorf if A is admissible. We shall assume in the following that any set of sequences A that we consider is admissible. A will be called trivial if it consists exactly of all finite sequences; in this case $\mathcal{P} = \mathcal{E}$.

PROPOSITION 6. *$\mathcal{P}$ is a complete locally convex Hausdorf topological vector space.*

Proof. Everything is obvious except the completeness of $\mathcal{P}$. Let ϕ be a Cauchy filter base in $\mathcal{P}$; since the topology of $\mathcal{P}$ is stronger than that of $\mathcal{E}$, ϕ converges to some element $f \in \mathcal{E}$. We claim that $f \in \mathcal{P}$ and ϕ converges to f in the topology of P.

We know that for any compact set $K \subset R$, for $f_\alpha \in \phi$, $f_\alpha \to f$, we have $\sum | a_n (d^n f_\alpha / dx^n)(x) |$ converges uniformly for all α and for $x \in K$; we claim it converges to $\sum | a_n (d^n f/dx^n)(x) |$. If we write $b_\alpha{}^n(x) = a_n f_\alpha{}^{(n)}(x)$, and $b^n(x) = a_n f^{(n)}(x)$, then the above is the statement that the conditions $b_\alpha{}^n(x) \to b^n(x)$ uniformly for $x \in K$, $\sum | b_\alpha{}^n(x) |$ converges uniformly for all α and for $x \in K$, imply $\sum | b^n(x) | < \infty$ and $\sum | b_\alpha{}^n(x) |$ converges to $\sum | b^n(x) |$ uniformly for $x \in K$. This is seen as follows:

Given any n_0 however large, we can find a cofinal set of α for which $| b_\alpha{}^n(x) - b^n(x) | \leqq 1/n_0$ for $n \leqq n_0$ and all $x \in K$. Thus,

$$\begin{aligned} \sum_{n \leqq n_0} | b^n(x) | &\leqq \sum_{n \leqq n_0} | b_\alpha{}^n(x) | + \sum_{n \leqq n_0} | b_\alpha{}^n(x) - b^n(x) | \\ &\leqq 1 + \sum_n | b_\alpha{}^n(x) | \\ &\leqq \text{const.}, \end{aligned}$$

where the constant is independent of n_0.

Finally, it is immediate that $\sum | a_n ((d^n f_\alpha / dx^n)(x) - (d^n f / dx^n (x))) | \to 0$. A similar argument works for the derivatives of f and gives our result.

In dealing with the Fourier transform, it is best to consider the Fourier transform of $\mathcal{P}'$ which is the dual of $\mathcal{P}$ with the topology of uniform convergence on the bounded sets of $\mathcal{P}$. For the Fourier transform of $\mathcal{P}'$ is, in general, a space of entire functions which can be described explicitly in many cases (compare Ehrenpreis [1], [3], and [8]). In fact, in many cases we get again a space which can be described by infinite derivatives.

We shall now consider several examples of spaces $\mathcal{P}$.

Hypothesis I. (α). The sequence $\{a_j\}$ belongs to A if $a(z) = \sum a_j z^j$ is an entire function of exponential type.

(β) If $\{a_j\} \in A$ and $c_j = O(1 + p^j)$ for some p, then $\{ \sum_{i=m}^{n} c_j a_{j-i} l^i / i! \}$ is in A for any l whenever $0 \leqq m \leqq n \leqq j$.

(γ). For any $f \in \mathcal{P}$, the series $\sum f^{(j)} X^j / j!$ converges to f in the topology of $\mathcal{P}$.

From Hypothesis I (α) it follows easily that all the functions in P are entire functions. Moreover, the topology of $\mathcal{P}$ is stronger than the topology of the space $\mathcal{H}$ of entire functions on the complex plane (see Ehrenpreis [5]).

Now, for any $S \in \mathfrak{P}'$, we define the Fourier transform $T = \mathfrak{F}(S)$ as the formal power series $T(z) = \sum T_j z^j$, where $T_j = S \cdot i^j X^j / j!$. In most cases T will be an analytic function. We denote by $\hat{\mathfrak{P}}'$ the space of Fourier transforms of $\mathfrak{P}'$ with the topology to make $\mathfrak{F}$ a topological isomorphism.

For any set A of sequences we denote by A^{-1} the set of all sequences $\{b_j\}$ such that $\sum |b_j a_j| < \infty$ for all $\{a_j\} \in A$. It is clear that A^{-1} is always admissible.

THEOREM 16. *Let A satisfy Hypothesis* I. *Then the space $\mathfrak{P}'$ is the space of infinitely differentiable functions defined by the operators D^b for $b \in A^{-1}$.*

Proof. First we note that, for any $b = \{b_j\} \in A^{-1}$, we have $\{b_j(1+j^2)X^j\}$ is bounded in the topology of $\mathfrak{P}$. For, given any $\{a_j\} \in A$ and any interval $[-l \leqq x \leqq l]$ in R, $(l \geqq 1)$, we have

$$\sup_{|x| \leqq l} |(1+j^2) a_j b_j |x|^j| = (1+j^2) |a_j b_j| l^j.$$

Now, by Hypothesis I(β), $\{a'_j\} = \{\sum_{i=0}^{j} (1+j^2) |a_{j-i}| l^i / i!\}$ is again in A, so that

$$\sup_{|x| \leqq l} |\{D^a[(1+j^2) b_j X^j]\}(x)| \leqq \sum_{i=0}^{j} (1+j^2) |b_j a_{j-i} j! l^i| / i!$$
$$= j! |b_j| (i + j^2) \sum_{i=0}^{j} |a_{j-i}| l^i / i!$$
$$= |b_j a_j'| j!.$$

Now, by hypothesis, $|b_j a_j'|$ is bounded in j. Thus,

$$\sup_{|x| \leqq l} |[D^a(b_j X^j / j!)](x)| \leqq \text{const.} / (1+j^2)$$

which is the desired result.

It follows that, for any $S \in \mathfrak{P}'$, $\{S \cdot (1+j^2) b_j i^j X^j / j!\} = \{(1+j^2) b_j T_j\}$ is a bounded set of complex numbers. Thus, $\sum |b_j T_j| < \infty$. It is also clear from the above that $\sum |b_j T_j|$ is uniformly bounded for T in any bounded set of $\hat{\mathfrak{P}}'$.

Conversely, suppose that T has the property that $\sum |b_j T_j| < \infty$ for any $\{b_j\} \in A^{-1}$; we want to show that $T \in \mathfrak{P}'$. For any $f \in \mathfrak{P}$, write $f(z) = \sum f_n z^n$, where, by hypothesis, the series converges to f in the topology of E. Then we define S by $S \cdot f = \sum f_n T_n (-i)^n n!$. We must show, of course, that this series converges. But we know that $\sum |a_n f_n n!|$ converges for any $\{a_n\} \in A$, by the definition of $\mathfrak{P}$.

LEMMA 10. *$(A^{-1})^{-1} \subseteq A$ for any admissible A.*

Lemma 10 is an immediate consequence of the definitions.

From Lemma 10, it follows that $\{(-i)_n T_n\} \in A$, and this implies that $f \to \sum f_n T_n (-i) n!$ defines a continuous linear function L on $\mathfrak{P}$. It is clear that the Fourier transform of L is just T, and this completes the proof of Theorem 16.

We have still to prove the statement in the theorem about the topology of $\hat{\mathfrak{P}}'$, but this can be accomplished by the above methods.

We want to use our theory of infinite derivatives to describe the topology of functions which are analytic on an arbitrary set B in the complex plane. The method is easily extended to sets in complex affine space of n dimensions. Now, if B is open, the compact-open topology is obviously the most natural one. For a more general class of B, a natural topology has been constructed by Van Hove (see Van Hove [1], Waelbroeck [1], Grothendieck [1], [2], Köthe [2]). This is defined as follows: Let $B_1, \cdots, B_r, \cdots$ be a sequence of open neighborhoods of B with $B_{j+1} \subset B_j$, $\cap B_j = B$ and each B consists of only a finite number of connected components each of which meets B. Let $\mathcal{H}(B_j)$ denote the space of functions which are analytic on B_j with the compact-open topology. Then we define $\mathcal{H}(B)$ as the inductive limit of the spaces $H(B_j)$ (see Köthe [1]), that is, $f \in \mathcal{H}(B)$ means that f is analytic on some neighborhood of B. $\mathcal{H}(B)$ is given the strongest locally convex topology which makes the natural maps $\mathcal{H}(B_j) \to \mathcal{H}(B)$ continuous.

Our definition of the topology by means of infinite derivatives is superior to the Van Hove topology because it is intrinsic, that is, it is defined in terms of the set alone without using the fact that it is a subset of the complex plane. Because of this, we are able to use our methods to define the topology on the real analytic functions on a real analytic manifold (with singularities). In addition, our method leads to the definition of the Fourier transform on these spaces. We hope to discuss these notions in detail in a future publication.

We shall change our previous notations slightly for convenience: We denote by $\mathcal{E}$ the space of indefinitely differentiable functions in the complex $z = x + iy$ plane with the Schwartz topology (Schwartz [1]). For B any subset of the plane, let $\bar{B}$ denote the closure of B. We also define $A = \{a_n\}$ such that

(54) $$a_n = O(\epsilon^n / n!) \text{ for any } \epsilon > 0.$$

Definition. Two functions which are analytic on a neighborhood of B are called equivalent if they coincide on a neighborhood of B. An equivalence class of functions analytic on neighborhoods of B is called an analytic function on B.

We have the obvious

LEMMA 11. *Let f_1 and f_2 be equivalent functions which are analytic on B. Then for any n and any $z_0 \in B$,*

$$(d^n f_1/dz^n)(z_0) = (d^n f_2/dz^n)(z_0).$$

Thus we can make the following

Definition. $\mathfrak{H}(B)$ is the space of analytic functions on B. A fundamental system of neighborhoods N of zero in $\mathfrak{H}(B)$ is defined as follows: Let K be a compact subset of B and let $\{a_n\} \in A$. Then N consists of all $f \in \mathfrak{H}(B)$ which satisfy

$$\max_{z \in K} \sum |a_n f^{(n)}(z)| \leqq 1. \tag{55}$$

PROPOSITION 7. *The following three topologies on the set of functions of $\mathfrak{H}(B)$ are equivalent:*

1. *The topology of $\mathfrak{H}(B)$.*

2. *The topology defined by the semi-norms*

$$\max_{n,z} a_n |f^{(n)}(z)|$$

for $\{a_n\} \in A$.

3. *The topology defined by the semi-norms*

$$\sum a_n \max_z |f^{(n)}(z)|$$

for $\{a_n\} \in A$.

Proof. It is clear that of the three topologies, 3 is the strongest and 2 is the weakest; thus we have to show that 2 is stronger than 3. Now, if $\{a_n\} \in A$, then so is $\{a_n n^2\}$. Thus, if $b > 0$ is properly chosen, any $f \in H(B)$ which satisfies $\max_z (a_n n^2) |f^{(n)}(z)| \leqq 1$ must satisfy $\sum a_n \max_z |f^{(n)}(z)| \leqq b$. Thus Proposition 7 is proven.

PROPOSITION 8. *Assume B possesses the following topological properties:*

1. *Every connected component of B is open in B.*

2. *Every connected component of B is analytically arcwise connected, that is, any two points belonging to the same component can be joined by a real analytic curve in B.*

3. *For each $z \in B$ let $U(z)$ be an open set in the complex plane. Then we can find a collection of sets $\{U_\alpha\}$ which are open in the complex plane*

and cover B such that each U_α is contained in some $U(z)$ and, moreover, if $U_\alpha \cap U_{\alpha'} \neq \phi$, $B \cap U_\alpha \cap U_{\alpha'} \neq \phi$.

Then $\mathfrak{H}(B)$ is a complete, Hausdorf, locally convex topological algebra. If B is open, then the topology of $\mathfrak{H}(B)$ is the compact-open topology.

Remark. Hypothesis 2 can be weakened to: Any two points in the same component can be joined by a piecewise analytic curve in B, and the proof is essentially the same as that given below. However, I do not know of Proposition 8 is true for an arbitrary set B.

Proof. It is clear that $\mathfrak{H}(B)$ is a locally convex Hausdorf topological vector space. To show the completeness of $\mathfrak{H}(B)$ we need the following

LEMMA 12. *Let $f^\alpha(z) = \sum (f^\alpha{}_n/n!)z^n$ be a formal power series with the property that $\sum |f^\alpha{}_n a_n|$ are uniformly bounded in α whenever $a_n = O(\epsilon^n/n!)$ for any $\epsilon > 0$. Then all $f^\alpha(z)$ are analytic in a fixed neighborhood of $z = 0$.*

Proof of Lemma. Assume that f^α is not analytic in a fixed neighborhood of $z = 0$. Then we can find an infinite sequence of positive numbers $n_j \to \infty$ and a sequence $\{\alpha_j\}$ such that

$$|f^{\alpha_j}{}_{n_j}| \geqq n_j!\, j^{n_j}.$$

Now, let

$$a_n = \begin{cases} j^{-n}/n! & \text{when } n = n_j \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $a_n = O(\epsilon^n/n!)$ for any $\epsilon > 0$, but

$$\sum |a_{n_j} f^{\alpha_j}{}_{n_j}| = \sum |f^{\alpha_j}{}_{n_j}|\, j^{-n_j}/n_j!$$
$$\geqq \sum 1 = \infty.$$

This concludes the proof of the lemma.

Proof of Proposition continued: Let $\{f^\alpha\}$ be a Cauchy filter base in $\mathfrak{H}(B)$; then f^α clearly converges to a function f which is continuous on B and is analytic at each interior point of B. For each n we define the continuous function $f_n(z) = \lim (d^n/dz^n) f^\alpha(z)$. For each $z_0 \in B$ we claim that the formal power series $\sum f_n(z_0)(z - z_0)^n$ converges in the neighborhood of z_0. For simplicity of notation we assume that $z_0 = 0$. Now, reasoning as in the proof of Proposition 6 we deduce that $\sum |f_n(0) a_n| < \infty$ whenever $\{a_n\} \in A$. By Lemma 12 we see that $\sum f_n(0) z^n$ is analytic in the neighborhood of $z = 0$.

Now, we have difficulty in constructing the limit of f^α because $N(z_0)$ and $N(z_1)$ may overlap without $\sum f_n(z_0)(z - z_0)^n$ and $\sum f_n(z_1)(z - z_1)^n$ being

equal in the intersection. However, by a simple argument we can show that we can choose neighborhoods $N'(z) \subset N(z)$ for any $z \in B$ with the additional property that $N'(z_0) \cap N'(z_1)$ is empty if z_0 and z_1 do not belong to the same connected component of B; namely, we just make sure that $N'(z)$ is contained in the circle, center z, radius less tha none-third the distance from z to the complement in B of the connected component of B containing z. The positivity of this distance is a result of the fact that z cannot be a limit point of points of B which do not lie in the same conected component, since the components are assumed to be open. By our assumptions on B we may also assume that $N'(z)$ have the property that if $N'(z) \cap N'(z') \neq \phi$ then $B \cap N'(z) \cap N'(z') \neq \phi$. (Of course, $N'(z)$ are open in the complex plane and cover B but $N'(z)$ are defined only for some z.)

Call $N = \bigcup_{z \in B} N'(z)$ and define g on N by $g(z) = \sum f_n(z_0)(z - z_0)^n/n!$ for $z \in N(z_0)$. We have three things to show: a. $g = f$ on B. b. g is well-defined. c. g is analytic on N.

Proof of a. *Let* $z_1 \in B$, then z belongs to some $N'(z_0)$. If $z_1 = z_0$ then certainly $f(z_1) = g(z_1)$. If $z_1 \neq z_0$ then by construction there exists a real analytic curve Γ lying in B and joining z_1 and z_0. It is a simple matter using integration on Γ to show that f is an indefinitely differentiable function on Γ and for all n we have $f_n(z) = (d^n/dz^n)f(z)$ for $z \in \Gamma$, where $d^n/dz^n f$ is defined by using difference quotients on Γ only; that is,

$$(df/dz)(z_2) = \lim_{z \in \Gamma,\, |z - z_2| \to 0} (f(z_2) - f(z))/(z_2 - z).$$

Moreover, since Γ is compact, the definition of our topology shows that for any $\{a_n\} \in A$ we must have $\sum | a_n f_n(z) |$ uniformly bounded for $z \in \Gamma$. Lemma 12 then tells us that there is a $\delta > 0$ so that all the power series $\sum f_n(z)(z' - z)^n/n!$ converge uniformly for $|z' - z| \leqq \delta$ and for $z \in \Gamma$. We now apply Pringsheim's theorem (see Mandelbrojt [2]): This tells us that f is real analytic on Γ. (Strictly speaking, Pringsheim's theorem is proven only for Γ a segment of the real axis, but there is no difficulty in extending the proof to any real analytic curve.)

Now, it is clear that g and f both have all their derivatives equal at z_0. Thus, since g and f are real analytic on Γ they are equal for all points of Γ. Thus, $g(z_1) = f(z_1)$ which is the desired result.

Proof of b. Let z_0, z_0' be points in B such that $N'(z_0) \cap N'(z_0')$ is not empty. Then by construction, $B \cap N'(z_0) \cap N'(z_0') \neq \phi$, so let $z_1 \in B \cap N'(z_0) \cap N'(z_0')$. Then we can join z_1 to z_0 and z_1 with analytic arcs

Γ_1, Γ_2 respectively. By a. above, $Cf_n(z_0)(z-z_0)^n/n!$ is equal to f on $(\Gamma_1 \cup \Gamma_2) \cap N'(z_0) \cap N'(z_0')$ and so is also equal to $\sum f_n(z_0')(z-z_0)^n/n!$. Since $\Gamma_1 \cup \Gamma_2$ is an arc and $N'(z_0) \cap N'(z_0')$ is open, the two functions

$$\sum f_n(z_0')(z-z_0')^n/n! \text{ and } \sum f_n(z_0)(z-z_0)^n/n!$$

must be equal on $N'(z_0) \cap N'(z_0')$. This proves that g is well defined.

Proof of c. This is clear from the definition.

It remains to show that f^α converges to f in the topology of $\mathfrak{H}(B)$ but this is clear. Thus, $\mathfrak{H}(B)$ is complete.

We show next that $\mathfrak{H}(B)$ is a topological algebra. This follows without difficulty from Leibnitz's formula for the derivative of a product:

$$(d^n/dx^n)(fh) = \sum_{j \leqq n} C_j{}^n f^{(j)} h^{(n-j)}.$$

Thus, if $a_n \geqq 0$,

$$\begin{aligned} \sum_n a_n \,|\, (d^n/dx^n)(fh) \,| &\leqq \sum_n \sum_{j \leqq n} a_n C_j{}^n \,|f^{(j)}|\,|\,h^{(n-j)}\,| \\ &= \sum_j \sum_k a_{j+k} C_j{}^{j+k} \,|\, f^{(j)} \,|\,|\, h^{(k)} \,|. \end{aligned} \tag{56}$$

Let us note that for $b_j \geqq 0$,

$$(\sum b_j \,|\, f^{(j)} \,|)(\sum b_k \,|\, h^{(k)} \,| = \sum_{j,k} b_j b_k \,|\, f^{(j)} \,|\,|\, h^{(k)} \,|.$$

Thus we can make the left side of (56) small if we make $a_{j+k} C_j{}^{j+k} \leqq b_j b_k$ for appropriate $\{b_j\}$.

Now, $a_{j+k} = O(\epsilon^{j+k}/(j+k)!)$ for any $\epsilon > 0$. Thus

$$\begin{aligned} a_{j+k} C_j{}^{j+k} &= O(\epsilon^{j+k}(j+k)!/(j+k)!j!k!) \\ &= O[(\epsilon^j/j!)(\epsilon^k/k!)] \end{aligned} \tag{57}$$

for any $\epsilon > 0$.

Using (57) we define $\{b_j\}$ as follows: Let $L = \max(j!a_j, 1)$. For each $l \geqq 1$, let p_l be chosen so large that $a_j \leqq K(1/l)^j(1/j!)$ for $j \geqq p_l$. Define $b_j = L^{\frac{1}{2}}(1/l)^j(1/j!)$ for $p_l \leqq j < p_{l+1}$. Then (56) and (57) show that the conditions

$$\max_{x \in K} \sum |\, b_j f^{(j)}(x) \,| \leqq 1, \qquad \max_{x \in K} \sum |\, b_j h^{(j)}(x) \,| \leqq 1$$

imply

$$\max_{x \in K} \sum |\, a_j (fh)^{(j)}(x) \,| \leqq 1$$

which proves that $\mathfrak{H}(B)$ is a topological algebra.

If B is open, then the topology of $\mathfrak{H}(B)$ is the compact-open topology

as is readily verified by means of Cauchy's integral. This completes the proof of Proposition 7.

In general, we do not know if the topology of $\mathcal{H}(B)$ is the same as the Van Hove topology; we shall give some examples later in which the two topologies are the same.

PROPOSITION 9. *Let h be a complex analytic mapping of B into B_1, that is, $h \in H(B)$ and $h(B) \subset B_1$. Define $h^*: H(B_1) \to H(B)$ by $h^*(f)(x) = f(h(x))$. Then h^* is a continuous linear map.*

Proof. h^* is clearly linear so we need verify at zero only. Let K be a compact set in B; since h is continuous, $h(K)$ is compact. Let $\{a_j\}$ be a sequence satisfying (54); let N be the set of $g \in H(B)$ which satisfy

$$\max_{x \in K} \sum a_j \, | \, g^{(j)}(x) \, | \leqq 1. \tag{58}$$

Then we want to find a sequence $\{b_j\}$ satisfying (54) such that $f \in H(B_1)$,

$$\max_{x \in h(K)} \sum b_j \, | \, f^{(j)}(x) \, | \leqq 1 \tag{59}$$

should imply $h^*f \in N$.

The sequence $\{b_j\}$ can be constructed by a method which is essentially the same as the classical proofs by power series methods that an analytic function of an analytic function is analytic. We shall omit the details.

We wish to give some examples:

Example 1. *Functions analytic at the origin.* We denote the space of functions analytic at the origin by $\mathcal{B}$. We show that the topology of $\mathcal{B}$ is the same as that of Van Hove. Let $\{a_n\}$ be a sequence of positive numbers such that $a_n = O(\epsilon^n/n!)$ for any $\epsilon > 0$, and let N be the set of $f \in \mathcal{B}$ satisfying $\sum | \, a_n f^{(n)}(0) \, | \leqq 1$. Suppose there exists a sequence $\{n_q\}$ with $n_0 = 0$ so that

$$a_n = 2^q q^{-n}/n! b_q \text{ for } n_{q-1} \leqq n < n_q, \, q \geqq 1. \tag{58}$$

We can write

$$f(x) = \sum_{q=1}^{\infty} 2^q f_q(x), \tag{59}$$

where $f_q(x) = 2^q \sum_{n_{q-1}}^{n_q-1} f_n x^n$; the series on the right clearly converges in a neighborhood of zero. Moreover, we have for $| \, x \, | \leqq q^{-1}$,

$$
\begin{aligned}
|f_q(x)| &\leqq 2^q \sum_{n=n_{q-1}}^{n_q-1} |f_n|\, q^{-n} \\
&= b_q \sum_{n=n_{q-1}}^{n_q-1} |f_n|\, a_n n! \\
&\leqq b_q \sum_{n=0}^{\infty} |f_n|\, a_n n! \\
&= b_q \sum_{n=0}^{\infty} |f^{(n)}(0)|\, a_n \\
&\leqq b_q.
\end{aligned}
$$

Thus, $|f_q(x)| \leqq b_q$ for $|x| \leqq q^{-1}$.

Now, suppose we start with a closed convex neighborhood N of zero in $\mathcal{B}$ in the Van Hove topology. Then for each $q > 0$ there is a $b_q > 0$ so that $\mathcal{B}$ contains the set of f which are analytic in $|x| \leqq q^{-1}$ and satisfy $|f(x)| \leqq b_q$ for $|x| \leqq q^{-1}$. We can clearly choose a sequence $\{n_q\}$ so that if we define a_n by (58), then $a_n = O(\epsilon^n/n!)$ for any $\epsilon > 0$. (It suffices to take $n_{q-1} > 2^q b_q^{-1}$ for all $q > 1$.) Thus the neighborhood M of zero in $\mathcal{B}$ defined by $\sum a_n |f^{(n)}(0)| \leqq 1$ has, by the above, the following property: each $f \in M$ can be written in the form $\sum_{q=1}^{\infty} 2^{-q} f_q$, where $f_q \in \mathcal{B}$. It is readily verified that the series $\sum 2^{-q} f_q$ converges in the topology of Van Hove. Since $\mathcal{B}$ is closed and convex by construction, this means that $f \in N$ which proves Proposition 9. The topology of $\mathcal{B}$ is the same as the Van Hove topology.

Example 2. Functions analytic in the closed unit disc. Let us denote by K the unit disc, that is, the set of x with $|x| \leqq 1$.

THEOREM 17. *The following three topologies on $\mathcal{H}(K)$ are equivalent:*

(1) *The topology of $\mathcal{H}(K)$.*

(2) *The Van Hove topology on K.*

(3) *The topology defined by the semi-norms $\sum b_n |f^{(n)}(0)|$, where $\{b_j\}$ is a sequence of positive numbers satisfying $b_n = O((1+\epsilon)^n/n!)$ for any $\epsilon > 0$.*

Proof. Exactly as in the proof of the previous Proposition 9 we can show that the topology described in (3) is stronger than the Van Hove topology.

If U is any open set containing K and if β is bounded in $\mathcal{H}(U)$, then β is clearly bounded in the topology (3). Thus, by general properties of the Van Hove topology, the toplogoy (2) is stronger than (3); hence, the topologies (2) and (3) are the same.

On the other hand, the Van Hove topology is stronger than the topology of $\mathcal{H}(K)$; Theorem 7 will thus be proven if we can show that topology (1) is stronger than (3). Now, for any function $f \in \mathcal{H}(K)$, f defines a function in L_2 of the unit circle. We have clearly (normalizing the measure so the unit circle gets measure 1)

(60) $$[\int |f(e^{i\theta})|^2 \, d\theta]^{\frac{1}{2}} \leqq \max_{|x| \leqq 1} |f(x)|.$$

By Parseval's theorem the left side of (60) is $\sum |f_n|^2$. Thus we see that

(61) $$\max_{|x| \leqq 1} |f(x)| \geqq [\sum |f_n|^2]^{\frac{1}{2}}.$$

By Schwart's inequality, $\sum |f_n|/(1+n^2) \leqq \text{const}\, [\sum |f_n|^2]^{\frac{1}{2}}$. Combining this with (61) we deduce

(62) $$\max_{|x| \leqq 1} |f(z)| \geqq \text{const} \sum |f_n|/(1+n^2).$$

Now, let $\{a_n\}$ be a given sequence satisfying $a_n = O(\epsilon^n/n!)$ for all $\epsilon > 0$. We consider the set of f for which $\sum a_j \max\limits_{x \in K} |f^{(j)}(x)| \leqq 1$. For each j we have by (62)

$$\max_{|x| \leqq 1} |f^{(j)}(x)| \geqq \text{const} \sum_{n \geqq j} |f_n| n!/(1+n^2)(n-j)!.$$

Thus,

$$\begin{aligned} 1 &\geqq \sum_j a_j \sum_{n \geqq j} |f_n| n!/(1+n^2)(n-j)! \\ &= \sum c_n |f_n| n! = \sum c_n |f^{(n)}(0)| \end{aligned}$$

say, where

(63) $$c_n = (1+n^2)^{-1} \sum_{j \leqq n} a_j/(n-j)!.$$

The binomial expansion $(1+\alpha)^n = \sum\limits_{j \leqq n} \alpha^j n!/j!(n-j)!$ shows that

$$c_n = O((1+\epsilon)^n/n!) \text{ for all } \epsilon > 0.$$

We are not finished, however! Given a sequence $\{b_n\}$ satisfying $b_n = O((1+\epsilon)^n/n!)$ for all $\epsilon > 0$ we have to produce a sequence $\{a_n\}$ satisfying $a_n = O(1+\epsilon)^n/n!)$ for all $\epsilon > 0$ so that for the corresponding sequence $\{c_n\}$ we have $b_n \leqq c_n$. The construction of $\{a_n\}$ is as follows: For each $q \geqq 1$ we define an integer d_q: $d_q \geqq 1$ is defined so that for $n \geqq d_q$ we have $b_n \leqq (1+1/q)^n/n!(1+n^2)$. d_0 is defined to be zero. We may clearly assume that $b_n \leqq 1/n!(1+n^2)$ for all n. Then we define

(64) $$a_n = q^{-n}/n! \text{ for } d_{q-1} \leqq n < d_q.$$

For $n \geqq d_q$, we have by (64), $a_n \geqq q^{-n}$. Thus, for $n \geqq d_q$,

$$\begin{aligned} c_n &= n!(1+n^2)^{-1} \sum_{j \leqq n} a^j/(n-j)! \\ &\geqq n!(1+n^2)^{-1} \sum_{j \leqq n} q^{-j}/(n-j)!j! \\ &= (1+n^2)^{-1}(1+1/q)^{-n} \\ &\geqq b_n. \end{aligned}$$

This completes the proof of Theorem 17.

Example 3. *Functions analytic on the unit circle.* We denote by $\dot{K}$ the unit circle, i. e. the boundary of K. Then we have

THEOREM 18. *The following topologies on $\mathfrak{H}(\dot{K})$ are equivalent:*

(1) *The topology of $\mathfrak{H}(\dot{K})$.*

(2) *The Van Hove topology on K.*

(3) *The topology defined by the semi-norms*

$$\sum b_n \mid f_n \mid, \textit{ where } f_n = \int_0^{2\pi} f(\theta) e^{-in\theta} \, d\theta$$

and where $\{b_n\}$ is a sequence of positive numbers satisfying $b_n = O(1+\epsilon)^n$ for any $\epsilon > 0$.

The proof is similar to the proof of the previous theorem and so will be omitted.

Similar results apply to the annulii

$$\alpha < | x | \leqq 1, \ \alpha \leqq | x | \leqq 1, \ \alpha \leqq | x | < 1$$

for any α with $0 \leqq \alpha < 1$. Now, by Proposition 9 our topology is invariant under conformal mappings which are real analytic on that part of the boundary of K which is in K; the same is true of the Van Hove topology (see Waelbruck [1]). Thus, the topology of $\mathfrak{H}(B)$ is the same as the Van Hove topology for B in case B is obtained from a domain of genus zero with real analytic boundary by adding certain parts of the boundary.

We do not know of any similar results for domains of genus > 1.

We conclude this section with a different application of the theory of infinite derivatives. This application is of great importance in obtaining very deep results on Cauchy's problem (see Ehrenpreis [10]).

For each r with $1 \leqq r < \infty$ we define ${}_r\mathcal{E}$ as the space of all $f \in \mathcal{E}$ for which the series $\sum a_n f^{(n)}$ converges in the space $\mathcal{E}$ whenever

$$a_n = O(\epsilon^n / \Gamma(rm)) \text{ for some } \epsilon > 0. \tag{65}$$

The topology of ${}_r\mathcal{E}$ is defined by means of the semi-norms $\sum a_n \max_{x \in K} |f^{(n)}(x)|$ for K a compact set in R and $\{a_n\}$ as above. The spaces ${}_r\mathcal{E}$ are easily shown to be complete topological vector spaces which are Schwartz spaces (hence reflexive). ${}_1\mathcal{E}$ is the space of entire functions and we shall write $\mathcal{E} = {}_\infty\mathcal{E}$. It is readily verified that ${}_r\mathcal{E}$ is metrizable. For $r \neq 1$ the spaces ${}_r\mathcal{E}$ bear the same relation to ${}_r\mathcal{D}$ that the space $\mathcal{E}$ does to the space $\mathcal{D}$.

${}_r\mathcal{E}$ is the dual of $\mathcal{E}$, ${}_r\hat{\mathcal{E}}'$ is the Fourier transform of ${}_r\mathcal{E}'$, as described above. For any $S \in {}_r\mathcal{E}'$, the Fourier transform $\mathcal{F}(S)$ is the function

$$\mathcal{F}(S)(z) = S \cdot \exp(iz \cdot)$$

for $z \in C$. It is easily seen that $\mathcal{F}(S)$ is an entire function of exponential type.

THEOREM 19. *${}_r\hat{\mathcal{E}}'$ consists of all entire functions F of exponential type which satisfy, for some A,*

$$|F(z)| = O(|P(z)|)\exp[A\,|Rz|^{r'} + |I(z)|], \tag{66}$$

where P is any polynomial, and where r' is defined by

$$r' = 1/r \text{ for } r \neq \infty, \quad \infty' = 0. \tag{67}$$

The topology of ${}_r\hat{\mathcal{E}}'$ is defined as follows: Let $H(z)$ be a positive continuous function on C such that all $B > 0$

$$\exp[B\,|Rz|^{r'} + |I(z)|] = O(H(z)). \tag{68}$$

Let N_H be the set of $F \in {}_r\hat{E}'$ for which

$$|F(z)| \leqq H(z)$$

for all $z \in C$. Then the sets N_H form a fundamental system of neighborhoods of zero in ${}_r\hat{\mathcal{E}}'$.

Proof. Let $S \in \mathcal{E}'$. Now, if a_n are positive numbers satisfying $a_n = O(\epsilon^n / \Gamma(rn))$ for some $\epsilon > 0$, then we have

$$\begin{aligned} \sum a_n\,|(d^n/dx^n)\exp(iz \cdot x)| &= |\exp(iz \cdot x)|\sum a_n\,|(iz)^n| \\ &\leqq \exp(|x|\,|\mathcal{I}(z)|)\sum a_n\,|z|^n. \end{aligned} \tag{69}$$

Now,

$$\begin{aligned}\sum a_n\,|\,z\,|^n &\leqq \text{const} \sum \epsilon^n\,|\,z\,|^n/\Gamma(rn+1)\\ &= \text{const} \sum (\epsilon\,|\,z\,|)^n/\Gamma(rn+1)\\ &= Q(\epsilon\,|\,z\,|),\end{aligned}$$

where

$$Q(z) = \sum z^n/\Gamma(rn+1).$$

For $x \geqq 0$, $Q(x)$ behaves like $\exp(x^{r'})$. This can be seen as follows:

$$\begin{aligned}\exp(x^{r'}) &= \sum_{n=0}^{\infty} x^{r'n}/n!\\ &= \sum_{rm=0}^{\infty} x^m/\Gamma(rm+1).\end{aligned}$$

LEMMA 13. *For $x \geqq 1$ we have*

$$\alpha Q(x) \leqq \exp(x^{r'}) \leqq \beta Q(2x) \tag{70}$$

for some constants α, β which depend only on r.

Proof of Lemma. We write first

$$\exp(x^{r'}) = \sum_{n=0}^{\infty} e_n(x),$$

where

$$e_n(x) = \sum_{j=[nr]}^{[(n+1)r]-1} x^{jr'}/j!, \tag{70}$$

where $[y]$ is the greatest integer $\leqq y$. Then for $x \geqq 1$, $[nr] \leqq j \leqq [(n+1)r]-1$ we have

$$x^{jr'} \leqq x^{(n+1)rr'} = x^{n+1}$$

while

$$\begin{aligned}j! &\geqq ([nr])!\\ &\geqq \Gamma(nr)\\ &\geqq \Gamma((n+1)r+1)/((n+1)r)^{r+2}.\end{aligned}$$

Thus, for $x \geqq 1$, we have

$$\begin{aligned}e_n(x) &\leqq (r+1)x^{n+1}((n+1)r)^{r+2}/\Gamma((n+1)r+1)\\ &\leqq \beta\alpha(2x)^{n+1}/\Gamma((n+1)r+1).\end{aligned}$$

Thus,

$$\begin{aligned}\exp(x^{r'}) &= \sum e_n(x)\\ &\leqq \beta \sum (2x)^n/\Gamma(nr+1)\\ &= \beta Q(2x).\end{aligned}$$

To prove the first inequality in (70), write

$$\exp(x^{r'}) = \sum e'_n(x),$$

where

$$e'_n(x) = \sum_{j=[nr]+1}^{[(n+1)r]} x^{jr'}/j!$$

and

$$e'_0(x) = \sum_{j=0}^{[r]} x^{jr'}/j!.$$

For $[nr]+1 \leqq j \leqq [(n+1)r]$ $(n>0)$ we have

$$x^{jr'} \geqq x^{nrr'} = x^n$$

while

$$\begin{aligned}j! &\leqq \Gamma((n+1)r+1)\\ &\leqq ((n+1)r)^{r+2}\Gamma(nr+1).\end{aligned}$$

Thus,

$$\begin{aligned}\exp(x^{r'}) &= \sum e'_n(x)\\ &\geqq (r+2)\sum_{n=0}^{\infty} x^n((n+1)r)^{-r-2}/\Gamma(nr+1)\\ &\geqq \alpha \sum (x/2)^n/\Gamma(nr+1)\\ &\geqq \alpha Q(x),\end{aligned}$$

which is the desired result.

Proof of Theorem continued. Since the cases $r=1,\infty$ are known (see Ehrenpreis [8]), we may assume $r \neq 1,\infty$. Let N be any neighborhood of zero in ${}_r\mathcal{E}$ on which S is bounded. By definition, there exist sequences $\{a_n^k\}$ $k=1,2,\cdots,l$ of positive numbers with $a_n^k = O(\epsilon^n/\Gamma(rn))$ for some $\epsilon>0$ and $p>0$ so that N contains the set of $f \in {}_r\mathcal{E}$ which satisfy $\max_{|x|\leqq p} \sum a_n^k |f^{(n)}(x)| \leqq 1$. Our above calculations show that for some $A>0$ we have

$$\exp(-A(|Rz|^{r'} + |Iz|)\exp(iz\cdot) \in N$$

for all complex numbers z. It follows immediately that $\mathfrak{F}(S)$ satisfies (66).

To prove that, conversely, any F satisfying (66) lies in ${}_r\mathcal{E}'$, we need the following lemma which can be proved in a manner similar to the proof of the corresponding result for the space ${}_\infty\mathcal{E}$ (see Ehrenpreis [1]):

LEMMA 14. *For $r \neq 1$, ${}_r\mathcal{E}'$ consists of all $S \in {}_r\mathcal{D}'$ for which the convolution $S^*f \in {}_r\mathcal{D}$ for any $f \in {}_r\mathcal{D}$. Consider ${}_r\mathcal{E}$ as a space of continuous linear maps (under convolution) of ${}_r\mathcal{D}$ into ${}_r\mathcal{D}$. Then the topology of ${}_r\mathcal{E}'$ is the compact-open topology for this set of maps.*

Now, it follows from Theorem 11′ that any function F satisfying (66) has the property that $FG \in {}_r\hat{\mathcal{D}}$ whenever $G \in {}_r\hat{\mathcal{D}}$. The fact that $f \in {}_r\hat{\mathcal{E}}'$ results from this by a simple argument (see the analogous argument in Ehrenpreis [1]).

Next, let N_H be a set as described in the statement of Theorem 16, where H satisfies (68). We want to show that N_H is a neighborhood of zero in ${}_r\hat{\mathcal{E}}'$. By a result of Grothendieck [1], ${}_r\hat{\mathcal{E}}'$ is bornologic so it is sufficient to prove that N_H swallows every bounded set, i.e., if B is bounded in ${}_r\hat{\mathcal{E}}'$ then for some $a > 0$ we have $aB \subset N_H$. This is proven by essentially the same argument as that used to prove that each $F \in {}_r\hat{\mathcal{E}}'$ satisfies (66).

The fact that the sets N_H form a fundamental system of neighborhoods of zero in ${}_r\hat{E}'$ is proven in essentially the same way as the corresponding result for the case $r = \infty$ (see Ehrenpreis [8]).

III. General remarks.

1. Let us consider, instead of the spaces ${}_r\mathcal{E}$, the spaces of functions $f \in \mathcal{E}$ for which the series $\sum a_n f^{(n)}$ converges in $\mathcal{E}$ whenever

$$a_n = O(\epsilon^n/\Gamma(rn)) \text{ for all } \epsilon > 0. \tag{71}$$

We give this space the usual topology and we obtain a topological vector space ${}^r\mathcal{E}$. In particular, ${}^1\mathcal{E}$ is the space of real analytic functions R. It seems to be a difficult task to describe the topology of the Fourier transform ${}^r\hat{\mathcal{E}}'$ of the dual of ${}^r\mathcal{E}$. One of the main difficulties is that no analog of Lemma 14 is possible for ${}^1\mathcal{E}$. On the other hand, a result Polyà (see Vl. Bernstein [1]) shows that ${}^1\mathcal{E}'$ consists of all entire functions of exponential type which are $O(\exp(\epsilon\,|\,x\,|))$ on the real axis for any $\epsilon > 0$.

2. A very difficult problem connected with the theory of infinite derivatives is the following: What kinds of conditions are necessary on the sets C_j, L_j in order that the space $\mathcal{B}$ should not be reduced to $\{0\}$. This problem is closely connected to the problems of the minimum modulus and quasi-analytic classes. Cf. Example 7 and Beurling [1].)

THE INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

R. Arens, [1] "Duality in linear spaces," *Duke Mathematical Journal*, vol. 14 (1947), pp. 787-794.

S. Banach, [1] *Théorie des Opérations Linéaires*, New York, 1955.

H. Bateman, [1] *Higher Transcendental Functions*, vol. I, II, III, New York, 1953-56.

Vl. Bernstein, [1] *Leçons sur les progrès récents de la séries de Dirichlet*, Paris, 1933.

A. Beurling, [1] "Some theorem on boundedness of analytic functions," *Duke Mathematical Journal*, vol. 16 (1949), pp. 355-359.

N. Bourbaki, [1] *Topologie Générale*, Livre III, Paris, 1940-49.
[2] *Intégration*, vol. XIII, Livre VI, Chapter III, Paris, 1953.

J. Dieudonné, [1] "Recent developments in the theory of locally convex vector spaces," *Bulletin of the American Mathematical Society*, vol. 59 (1953), pp. 495-512.

——— and L. Schwartz, [1] "La dualité dans les espaces ($\mathcal{F}$) et ($L\mathcal{F}$)," *Annales de L'Institut Fourier*, vol. 1 (1950), pp. 61-101.

L. Ehrenpreis, [1] "Analytic functions and the Fourier transform of distributions I," *Annals of Mathematics*, vol. 63 (1956), pp. 129-159.
[2] "——— II," *Transactions of the American Mathematical Society*, vol. 89 (1958), pp. 450-483.
[3] "Solutions of some problems of division I," *American Journal of Mathematics*, vol. 76 (1954), pp. 883-903.
[4] "——— II," *American Journal of Mathematics*, vol. 77 (1955), pp. 286-292.
[5] "Mean periodic functions I," *American Journal of Mathematics*, vol. 77 (1955), pp. 293-328. (Also Appendix, *ibid.*, pp. 731-733.)
[6] *Theory of distributions for locally compact spaces*, Memoirs of the American Mathematical Society, no. 21, 1956.
[7] "General theory of elliptic equations," *Proceedings of the National Academy of Sciences*, vol. 42 (1956), pp. 39-41.
[8] "Solutions of some problems of division III," *American Journal of Mathematics*, vol. 78 (1956), pp. 685-715.
[9] "Completely inversible operators," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 945-946.
[10] *Treatise on systems of convolution equations*, to appear.
[11] "Cauchy's problem for linear differential equations with constant coefficients," *Proceedings of the National Academy of Science*, vol. 42 (1956), pp. 642-646.
[12] "Solution of some problems of division IV" (to appear).

I. M. Gelfand and G. E. Silov, "Fourier transforms of rapidly increasing functions and questions of uniqueness in the solution of Cauchy's problem," *Uspekhi Matematičeskih Nauk*, vol. 8 (1953), pp. 3-54, *Translations of the American Mathematical Society*, vol. 5, pp. 221-274.

A. Grothendieck, [1] "Sur certains espaces de fonction holomorphes," I and II, *Journal für die reine und angewandte Mathematik*, vol. 192 (1953), pp. 35-64, and p. 77-95.

L. Hörmander, [1] "On the theory of general partial differential operators," *Acta Mathematica*, vol. 94 (1955), pp. 161-248.

[2] "La transformation de Laplace et le théorème de Paley-Wiener," *Comptes rendus Académie Sciences*, vol. 240 (1955), pp. 382-394.

[3] "Differentiability properties of solutions of systems of differential equations," *Arkiv för Matematik*, vol. 3 (1958), pp. 527-535.

G. Köthe, [1] "Über die Vollständigkeit einer Klasse lokalconvexer Räume," *Mathematische Zeitschrift*, vol. 52 (1950), pp. 627-630.

[2] "Dualität in der Funktiontheorie," *Journal für die reine und angewandte Mathematik*, vol. 191 (1953), pp. 30-49.

J. L. Lions, [1] "Supports dans la transformation de Laplace," *Journal d'Analyse Mathematique (Jerusalem)*, vol. 2 (1952-53), pp. 369-380.

G. Mackey, [1] "On convex topological linear spaces," *Transactions of the American Mathematical Society*, vol. 60 (1946), pp. 519-537.

S. Mandelbrojt, [1] *Séries Lacunaires*, Paris, 1936.

[2] *Les Séries Adherentes*, Paris, 1952.

R. E. A. C. Paley and N. Wiener, [1] *Fourier transforms in the complex domain*, New York, 1934.

H. Poincaré, [1] "Sur les fonctions à espaces lacunaires," *American Journal of Mathematics*, vol. 14 (1892), pp. 213-215.

A. C. Schaeffer, [1] "Entire functions and trigonometric polynomials," *Duke Mathematical Journal*, vol. 20 (1953), pp. 77-88.

L. Schwartz, [1] *Théorie des Distributions*, vols. I and II, Paris, 1951-52.

[2] *Etude des Sommes d'Exponentielles Réeles*, Paris, 1943.

[3] "Analyse et synthèse harmonique dans les espaces de distributions," *Canadian Journal of Mathematics*, vol. 3 (1951), pp. 503-512.

[4] "Théorie générale des fonctions moyenne-périodiques," *Annals of Mathematics*, vol. 48 (17947), pp. 857-929.

[5] "Transformation de Laplace des distributions," *Communications du Séminaire Mathématique de l'Université de Lund*, 1952, pp. 196-206.

E. C. Titchmarsh, [1] *The Theory of Functions*, Oxford, 1932.

[2] *Theory of Fourier Integrals*, Oxford, 1937.

L. Van Hove, [1] "Topology des espaces fonctionelles analytiques, et des groupes infinis de transformations," *Bulletin de l'Academic Belgique*, vol. 38 (1952), pp. 333-351.

L. Waelbroeck, [1] "Le calcul symbolique dans les algèbres commutatives," *Journal de Mathématiques Pures et Appliquées*, vol. 33 (1954), pp. 147-186.

A. Zygmund, [1] *Trigonometrical Series*, New York, 1952.

ON THE HILBERT-SIEGEL MODULAR SPACE.*

By WALTER L. BAILY, JR.†,‡

Introduction. Let $\mathfrak{S}_n$ be the space of complex, symmetric, $n \times n$ matrices $Z = X + iY$ with positive definite imaginary part Y, $Y \gg 0$, and let $\mathfrak{S}_n{}^p = \mathfrak{S}_n \times \cdots \times \mathfrak{S}_n$ be the product of p replicas of $\mathfrak{S}_n$. Let $Sp(n, R)$ be the group of $2n \times 2n$ real symplectic matrices. Then $Sp(n, R)$ is naturally homomorphic to a transitive group of complex analytic transformations of $\mathfrak{S}_n$, and therefore $(Sp(n, R))^p$ is (homomorphic to) a transitive group of complex analytic transformations of $(\mathfrak{S}_n)^p$. Let $\mathfrak{k}$ be a totally real algebraic number field of (absolute) degree p and let $\mathfrak{o}$ be the ring of integers in $\mathfrak{k}$. The group $Sp(n, \mathfrak{k})$ of points in $Sp(n, R)$ having coordinates in $\mathfrak{k}$ can be imbedded in $(Sp(n, R))^p$ by

$$i\colon M \to (M^{\sigma_1}, \cdots, M^{\sigma_p}),$$

where $\sigma_1 =$ identity, $\sigma_2, \cdots, \sigma_p$ are the distinct isomorphisms of $\mathfrak{k}$ into R. The group $\Gamma_{n,p}{}^* = i(Sp(n, \mathfrak{k}))$ is everywhere dense in the Lie group $(Sp(n, R))^p$, and therefore the orbit of any point of $\mathfrak{S}_n{}^p$ under $\Gamma_{n,p}{}^*$ is everywhere dense in $\mathfrak{S}_n{}^p$. Let $Sp(n, \mathfrak{o})$ be the subgroup of $Sp(n, \mathfrak{k})$ consisting of those M with coordinates in $\mathfrak{o}$ such that $\det M = 1$ and put $\Gamma_{n,p} = i(Sp(n, \mathfrak{o}))$. Then $\Gamma_{n,p}$ acts in a properly discontinuous manner on $\mathfrak{S}_n{}^p$ and is known as the Hilbert-Siegel modular group [10]. The quotient space $(\mathfrak{S}_n)^p/\Gamma_{n,p}$, denoted by $\mathfrak{V}_{n,p}$, has finite volume with respect to the invariant measure on $(\mathfrak{S}_n)^p$. The same thing will be true of any subgroup $\Gamma_{n,p}{}'$ of $\Gamma_{n,p}{}^*$ commensurable with $\Gamma_{n,p}$. We note in passing that if $\gamma \in \Gamma_{n,p}{}^*$, then $\gamma^{-1}\Gamma_{n,p}\gamma$ is commensurable with $\Gamma_{n,p}$. When no confusion can arise, we shall denote $\Gamma_{n,p}{}^*$, $\Gamma_{n,p}$, and $\Gamma_{n,p}{}'$ by $\Gamma_n{}^*$, Γ_n, and $\Gamma_n{}'$ respectively, or still more simply by Γ^*, Γ, and Γ'. The main purpose of our paper will be to show that each of the quotient spaces $(\mathfrak{S}_n{}^p)/\Gamma'$ can be compactified to a normal general analytic space, isomorphic to a projective variety. With a few important exceptions, our proof is quite similar to the treatment of the Siegel modular group ($p = 1$) [12], and therefore we shall in many cases simply refer the reader to [12] for the more or less formal

* Received January 9, 1959.

† This work was done while the author was an Alfred P. Sloan Research Fellow.

‡ The author wishes to express his thanks to T. I. Bartha for valuable criticism.

details of proofs, reserving our efforts for concentration on those aspects which apparently cannot be lifted trivially from the case of the Siegel modular group, $p=1$.

We note here that the set of abelian varieties whose multiplication ring is an order in $\mathfrak{k}$ may be identified (non-canonically) with $(\mathfrak{S}_n)^p$ (see [10, pp. 36-42]). It is this point of view that has motivated the approach in [10]. However, we shall not pursue this interesting fact any further here. We should also like to call attention to the (well-known) fact that the group of units of $\mathfrak{o}$ plays an important role in constructing the compactifications of the spaces $(\mathfrak{S}_n)^p/\Gamma'$; it might be of interest to examine this fact further, but we cannot contribute anything in this direction at present.

At this point we introduce certain notation which we have chosen to come as close as possible to that of [12]. First of all, if σ_l is one of the isomorphisms of $\mathfrak{k}$ into R, and if x is some quantity over $\mathfrak{k}$, then x^l shall denote the result of applying σ_l to x, while if $Z\in\mathfrak{S}_n{}^p$, Z^l shall denote the l-th component of Z in the product $\mathfrak{S}_n\times\cdots\times\mathfrak{S}_n$, $z_{ij}{}^l$ denoting the ij-th entry of the matrix Z^l. Then if M denotes a p-tuple of matrices, $\operatorname{tr}(M)=\sum_l(\sum_i m_{ii}{}^l)$. If S is a matrix over k, we write $S\gg 0$ if each of the matrices $S^1,\cdots,S^p$ is positive definite, and $S\geqq 0$ if the requirement of positive definiteness is replaced by positive semi-definiteness. Moreover,

$$N\det(CZ+D)=\prod_l\det(C^lZ^l+D^l),$$

and, in general, multiplicative quantities of Siegel's theory [14], such as $\det Y$, should be replaced by the absolute norms of those quantities, whereas additive quantities such as $ds^2=\operatorname{tr}(Y^{-1}dZY^{-1}dZ)$ should be replaced by the absolute traces of these quantities. Finally, "integer" will usually mean an element of $\mathfrak{o}$.

1. Reduction theory and fundamental open sets for Γ'. We wish to construct a fundamental open set for $\Gamma_{n,p}'$ in $\mathfrak{S}_n{}^p$, i.e., an open set B' in $\mathfrak{S}_n{}^p$ having finite invariant volume such that $\Gamma_{n,p}'B'=\mathfrak{S}_n{}^p$ and such that $\gamma B'\cap B'$ is non-empty for only a finite number of $\gamma\in\Gamma_{n,p}'$. For the convenience of the reader we indicate briefly the results of [8] and [10] which we shall need. Since a fundamental open set for Γ' can be constructed by taking the union of a finite number of fundamental open sets for Γ, we first construct a fundamental open set B for Γ.

Let E_{2m} be a $2m$-dimensional vector space over the rational numbers and let E_{2m} be supplied with a skew-symmetric bilinear form (x,y). The group

of linear automorphisms of E_{2m} leaving this bilinear form invariant is called the group of symplectic transformations of E_{2m} (with respect to the bilinear form). A subspace Q of E_{2m} is called a null space if $(x,y)=0$ for all $x,y\in Q$. A linear transformation A of E_{2m} is called symplectically self-adjoint if $(Ax,y)=(x,Ay)$, $x,y\in E_{2m}$. If ${}^t\mathfrak{A}$ is an algebra of symplectically self-adjoint transformations of E_{2m}, we denote by $S_{\mathfrak{A}}$ the group of integral symplectic transformations M of E_{2m} such that $M{}^tA={}^tAM$ for all ${}^tA\in{}^t\mathfrak{A}$. (Here ${}^tA$ is the transpose of A and ${}^t\mathfrak{A}$ is the algebra consisting of the transposes of elements of the algebra $\mathfrak{A}$.) Two maximal null spaces Q_1 and Q_2 ($\neq 0$) of E_{2m}, invariant under ${}^t\mathfrak{A}$, are called equivalent if there exists $M\in S_{\mathfrak{A}}$ such that $MQ_1=Q_2$.

A representation $\alpha\to\mathfrak{A}(\alpha)$ of $\mathfrak{k}$ by $m\times m$ matrices with entries from the field of rational numbers is called normal if the entries of $\mathfrak{A}(\alpha)$ are rational integers whenever $\alpha\in\mathfrak{o}$. The number of equivalence classes of normal representations (under unimodular equivalence) is finite, being bounded by $h^{m/p}$, where h is the class number of $\mathfrak{k}$. Using this fact, it is not hard to prove that if $\mathfrak{A}$ is a normal representation of $\mathfrak{k}$ by $2m\times 2m$ matrices A such that ${}^tA$ is symplectically self-adjoint, then the number of equivalence classes of maximal invariant null-spaces is finite.

An $r\times s$ matrix over $\mathfrak{k}$ may be viewed as a $pr\times ps$ matrix over the rational numbers. Let C and D be $n\times n$ matrices over $\mathfrak{o}$; the pair (C,D) is called symmetric if $C^tD=D^tC$, and primitive if for any non-singular matrix B over $\mathfrak{k}$, (BC,BD) integral implies $|N\det B|\geqq 1$. By a choice of integral basis in $\mathfrak{k}$, C and D may be viewed as $m\times m$ matrices with rational integral entries. Let L denote the m-dimensional vector sub-space of E_{2m} which the rows of (CD) span over the field of rational numbers. The condition $C^tD=D^tC$ says simply that this vector space L is a null space with respect to a certain skew-symmetric, bilinear form. The field $\mathfrak{k}$, which operates linearly on the vector space of dimension $2n$ over $\mathfrak{k}$, then possesses a natural representation as an algebra ${}^t\mathfrak{A}$ of symplectically self-adjoint transformations of E_{2m} (with respect to the above bilinear form), and $S_{\mathfrak{A}}$ is just the subgroup of the group of integral, unimodular, symplectic transformations of E_{2m} which arise in the obvious way from elements of $Sp(n,\mathfrak{o})$. The primitive pairs (C,D) and (C_1,D_1) are said to be equivalent if there exists $U\in Sp(n,\mathfrak{o})$ and a unimodular $n\times n$ matrix B (i.e., $N\det B$ is a unit), over $\mathfrak{k}$ such that $B(CD)U=(C_1D_1)$. Then it is easily seen that the primitive pairs (C,D) giving rise to the same maximal invariant null-space in E_{2m} are equivalent. Hence, there are only a finite number of equivalence classes of primitive pairs (C,D).

We now proceed ([10]) to construct a fundamental open set for $\Gamma_{n,p}$. If (C, D) is a primitive symmetric pair, define

$$\chi(C,D;Z) = |N \det(CZ+D)|.$$

If $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(n, \mathfrak{o})$,

$$i(M)(Z^1,\cdots,Z^p) = ((A^1Z^1+B^1)(C^1Z^1+D^1)^{-1},\cdots,(A^pZ^p+B^p)(C^pZ^p+D^p)^{-1}).$$

Let $\chi(M;Z) = \chi(C,D;Z)$. In the future, we shall use MZ to denote $i(M)Z$. If $\mu > 0$, define

$$\Omega(\mu) = \{Z \mid |\chi(C,D;Z)| > \mu \text{ for all symmetric, coprime pairs } C, D\}.$$

Using the fact that the number of equivalence classes of primitive symmetric pairs is finite, it is not hard to show that there exists $\mu_0 > 0$ and a finite number of transformations $M_1,\cdots,M_q \in Sp(n,\mathfrak{k})$ such that if $Z \in \mathfrak{S}_n{}^p$, then there exists $M \in Sp(n,\mathfrak{o})$ for which $M_\nu MZ \in \Omega(\mu_0)$ for some ν, $1 \leqq \nu \leqq q$.

If $Y = (Y^1,\cdots,Y^p)$, $Y^i = {}^tY^i \gg 0$, $i = 1,\cdots,p$, then each $Y^i = D^i[T^i]$, D^i being diagonal with entries $d_{jk}{}^i = \delta_{jk}d_j{}^i$ and T^i being unipotent triangular with entries $t_{jk}{}^i$ ($t_{jk}{}^i = \delta_{jk}$ if $k \leqq j$). If $t > 0$, define

$$Q(t) = \{Y \mid |t_{jk}{}^i| < t \text{ if } j > k,\ t^{-1}d_j{}^{i_1} < d_j{}^{i_2} < td_j{}^{i_1},$$
$$d_j{}^i < td_{j+1}{}^i, \text{ all } i, i_1, i_2, j\}.$$

According to Humbert [8], there exists $t_0 > 0$ and a finite number of non-singular matrices $A_1,\cdots,A_r \in GL(n,\mathfrak{k})$ such that every $Y = (Y^1,\cdots,Y^p)$ can be written as $Y'[A_\rho U]$ for some $Y' \in Q(t_0)$, $1 \leqq \rho \leqq r$, and U belonging to the group of unimodular matrices over $\mathfrak{o}$. Choose a basis $\omega_1,\cdots,\omega_p$ of the integers in $\mathfrak{k}$ and let $Q'(t)$ denote the set of $Z \in \mathfrak{S}_n{}^p$ such that $Y = \operatorname{Im} Z \in Q(t)$ and such that $\operatorname{Re} Z = X = (X^1,\cdots,X^p)$, where X^i, $1 \leqq i \leqq p$, can be written as $X^i = \sum_j \omega_j{}^i \Xi_j$, Ξ_j being a real symmetric matrix with entries $\xi_{j,k,l}$ satisfying $|\xi_{j,k,l}| < t$. For any μ, $t > 0$ let $\Omega = \Omega_n = \Omega(\mu, t) = \Omega(\mu) \cap Q'(t)$. Then there exists a constant $\lambda > 0$, $\lambda = \lambda(\mu, t)$, such that if $Z \in \Omega(\mu, t)$, we have $\operatorname{Im} Z = Y \gg \lambda E$.

Then from the results of [8] and [10], and the above, it follows that there exists a set $B(\Omega)$ consisting of a finite number of translates of Ω under elements of Γ^* such that $\Gamma_{n,p}B(\Omega) = \mathfrak{S}_n{}^p$ and such that $B(\Omega)$ meets only a finite number of its translates under $\Gamma_{n,p}$. Since it follows from the existence of the constant λ that $B(\Omega)$ has finite invariant volume (the invariant volume element is $N(\det Y^{-n-1}dXdY)$), we see that $B(\Omega)$ is a fundamental open

set for Γ. If Γ' is commensurable with Γ, the union $B'(\Omega)$ of a finite number of translates of $B(\Omega)$ under elements of Γ is a fundamental open set for Γ'.

We choose $\mu < \mu_0$, $t > t_0$ such that for each r, $0 \leqq r \leqq n$, the open set $\Omega_r(\mu, t) = \Omega_r$ in $\mathfrak{S}_r^p$ satisfies the same conditions with respect to Γ_r as $\Omega_n(\mu, t)$ does with respect to Γ_n, so that the union $B(\Omega_r)$ of a certain finite number of translates of Ω_r under elements of Γ_r^* will be a fundamental open set for Γ_r. Let $\mu_1 < \mu$, $t_1 > t$. We now define a topology on $\Omega_n(\mu_1, t_1) \cup \cdots \cup \Omega_0(\mu_1, t_1)$. If $Z_0 \in \Omega_r$, let $\mathcal{U}_r$ be a neighborhood of Z_0 in Ω_r and let $K > 0$. Define $\mathcal{U}_s = V^s(\mathcal{U}_r, K)$, $r \leqq s \leqq n$, to be the set of $\begin{pmatrix} Z_1 & Z_{12} \\ {}^tZ_{12} & Z_2 \end{pmatrix} \in \Omega_s(\mu_1, t_1)$ such that $Z_1 \in \mathcal{U}_r$ and $d_{r+1}{}^i > K$, $i = 1, \cdots, p$. Then by definition, $\mathcal{U} = \bigcup_{s=r}^{n} \mathcal{U}_s$ is one of a basis of neighborhoods of Z_0 in $\bigcup_{s=0}^{n} \Omega_s(\mu_1, t_1)$ (it may be verified as in [12, exposé 12] that this gives rise to a legitimate topology). Then we topologize $\bigcup_{s=0}^{n} \operatorname{clos}(\Omega_s(\mu, t)) \subset \bigcup_{s=0}^{n} \Omega_s(\mu_1, t_1)$ with the subspace topology.

Let $\rho\colon \mathfrak{S}_n^p \to \mathfrak{S}_n^p$ be defined by

$$\rho(Z^1, \cdots, Z^p) = (-(Z^1)^{-1}, \cdots, -(Z^p)^{-1}).$$

$\rho \in \Gamma_{n,p}$. Therefore $\rho(B(\Omega))$ is also a fundamental open set for $\Gamma_{n,p}$. $\rho(\Omega_n)$ is a bounded set in the $\frac{1}{2}pn(n+1)$-dimensional space of p-tuples of complex, symmetric, $n \times n$ matrices, and its closure there, $\operatorname{clos} \rho(\Omega_n)$, is naturally homeomorphic to $\operatorname{clos}(\Omega_n) \cup \cdots \cup \operatorname{clos}(\Omega_0)$ (this follows from [12, p. 12-04, Lemma 1, 1°]).

We denote by $\mathfrak{G}_r^n$ the subgroup consisting of those $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp(n, \mathfrak{k})$ such that $A = \begin{pmatrix} A_1 & 0 \\ A_{21} & A_2 \end{pmatrix}$, $B = \begin{pmatrix} B_1 & B_{12} \\ B_{21} & B_2 \end{pmatrix}$, $C = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}$, $D = \begin{pmatrix} D_1 & D_{12} \\ 0 & D_2 \end{pmatrix}$, where A_1, B_1, C_1, D_1 are $r \times r$ and A_2, B_2, and D_2 are $(n-r) \times (n-r)$. $\mathfrak{G}_r^n$ may be characterized as the smallest subgroup $\mathfrak{G}$ of $Sp(n, \mathfrak{k})$ with the property that if $\{Z_\nu\}$, $\{Z_\nu'\}$ are sequences in $\operatorname{clos} \Omega_n \subset \mathfrak{S}_n^p$ with limits $Z_0 \in \operatorname{clos} \Omega_r \subset \mathfrak{S}_r^p$, $Z_0' \in \operatorname{clos} \Omega_{r'}{}^p \subset \mathfrak{S}_{r'}{}^p$ such that $Z_\nu = MZ_\nu'$, $M \in \Gamma_{n,p}$ fixed, then $r = r'$ and $M \in \mathfrak{G}$ (see [12, p. 12-04, Lemma 1]). It is easily seen that $\pi\colon \begin{pmatrix} A & B \\ C & D \end{pmatrix} \to \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$ is a homomorphism of $\mathfrak{G}_r^n$ onto $\Gamma_{r,p}^*$. We denote the kernel of π by $\mathfrak{N}_r^n$. $\mathfrak{N}_r^n$ consists of all $M \in Sp(n, \mathfrak{k})$ of the form $M = \begin{pmatrix} {}^tU & TU^{-1} \\ 0 & U^{-1} \end{pmatrix}$, where $U \in GL(n, \mathfrak{k})$ is of the form $\begin{pmatrix} E & U_{12} \\ 0 & U_2 \end{pmatrix}$ and where T is a symmetric $n \times n$ matrix over $\mathfrak{k}$ of the form $T = \begin{pmatrix} 0 & T_{12} \\ {}^tT_{12} & T_2 \end{pmatrix}$. If M

belongs to a subgroup of $Sp(n, \mathfrak{k})$ commensurable with $Sp(n, \mathfrak{o})$, it is easy to see that some power of U must be in the group of unimodular matrices over $\mathfrak{o}$, and therefore $N \det U = \pm 1$.

If $\mathfrak{G}$ is a group of transformations of the space D_1 and τ a homeomorphism of D_1 onto the space D_2, we let $\mathfrak{G}^\tau = \tau\mathfrak{G}\tau^{-1}$.

By the mapping

$$\tau: (Z^j) \to ((E + iZ^j)(E - iZ^j)^{-1})$$

(the so-called "Cayley transformation") $\mathfrak{S}_n{}^p$ is transformed onto $\mathfrak{B}_n{}^p$, where $\mathfrak{B}_n$ is the "generalized unit disc" consisting of all symmetric complex matrices W such that $W\bar{W} \ll E$, and $\Gamma_{n,p}$ is transformed into the properly discontinuous group $\Gamma_{n,p}{}^\tau$ acting on $\mathfrak{B}_n{}^p$. $\tau(\rho(B(\Omega)))$ is evidently a fundamental open set for $\Gamma_{n,p}{}^\tau$. $Sp(n, \mathfrak{k})^\tau$ is an almost transitive (i.e., the orbit of each point is dense) group of transformations of $\mathfrak{B}_n{}^p$, and is also a group of continuous transformations of $\operatorname{clos}(\mathfrak{B}_n{}^p) = \mathfrak{A}_n{}^p$. As in [12, p. 12-15] we let

$$\mathfrak{A}_{n,r}{}^p = \{(W_j) \mid \operatorname{rank}(E - W_j\bar{W}_j) \leqq r\}$$
$$\mathfrak{B}_{n,r}{}^p = \{(W_j) \mid \operatorname{rank}(E - W_j\bar{W}_j) = r\}.$$

Each $\mathfrak{B}_{n,r}{}^p$ is stable under $Sp(n, \mathfrak{k})^\tau$, and the latter acts almost transitively on $\mathfrak{B}_{n,r}{}^p$. As in [12, p. 13-01] we may easily prove that

$$Sp(n, \mathfrak{k})^\tau \operatorname{clos}(\tau(\rho(B(\Omega)))) = \Gamma_{n,p}{}^\tau \operatorname{clos}(\tau(\rho(B(\Omega))))$$

(the operations of closure being with respect to the entire space of $n \times n$ complex, symmetric matrices). We denote $\Gamma_{n,p}{}^\tau \operatorname{clos}(\tau(\rho(B(\Omega))))$ by $\mathfrak{A}_n{}^*$ (there is no need to exhibit p explicitly here since the field $\mathfrak{k}$ is fixed throughout). We denote $\tau(\rho(\Omega))$ by $\sum$ and $\tau(\rho(B(\Omega)))$ by $B(\sum)$. Then $\operatorname{clos}(B(\sum))$ is the union of a finite number of translates of $\operatorname{clos}(\sum)$ by elements of $Sp(n, \mathfrak{k})^\tau$, $\operatorname{clos}(B(\sum)) = \bigcup_{i=1}^{s} \sigma_i \operatorname{clos}(\sum)$, $\sigma_i \in Sp(n, \mathfrak{k})^\tau$. We topologize $\operatorname{clos}(B(\sum))$ with the finest topology such that each of the mappings

$$\operatorname{clos}(\textstyle\sum) \to \sigma_i \operatorname{clos}(\textstyle\sum) \subset \operatorname{clos}(B(\textstyle\sum))$$

is continuous, and topologize $\mathfrak{A}_n{}^*$ with the finest topology such that each of the mappings

$$\operatorname{clos}(B(\textstyle\sum)) \to \gamma \operatorname{clos}(B(\textstyle\sum)) \subset \mathfrak{A}_n{}^*,$$

$\gamma \in Sp(n, \mathfrak{k})$, is continuous. Then as in [12, exposés 12 and 13] it is not

hard to see that $Sp(n,\mathfrak{k})^\tau$ acts as a group of continuous transformations o $\mathfrak{A}_n^*$. We let (as in [12, p. 12-15])[1]

$$\mathfrak{A}_{n,r}^* = \mathfrak{A}_n^* \cap \mathfrak{A}_{n,r}, \qquad \mathfrak{B}_{n,r}^* = \mathfrak{B}_{n,r} \cap \mathfrak{A}_n^*$$

$0 \leqq r \leqq n$. As previously remarked, the homeomorphism ρ of Ω_n onto $\rho(\Omega_n)$ may be extended to a homeomorphism, which we again denote by ρ, o $\bigcup_{s=0}^{n} \operatorname{clos}(\Omega_s)$ onto $\operatorname{clos}\rho(\Omega_n)$. Let C_r denote the connected component of $\mathfrak{B}_{n,r}^*$ containing $\tau(\rho(\Omega_r))$; then C_r is complex analytically isomorphic to $\mathfrak{S}_r^p$ the subgroup $(\mathfrak{G}_n^r)^\tau$ of $Sp(n,\mathfrak{k})^\tau$ acts almost transitively on C_r, and i $\sigma \in Sp(n,\mathfrak{k})^\tau - (\mathfrak{S}_n^r)^{\tau\rho}$, $C_r \cap \sigma C_r$ is empty. Moreover, if $\gamma \in \mathfrak{G}_n^r$, the actio of $\tau\rho\gamma(\tau\rho)^{-1}$ on C_r is the same as that of $\pi_r(\gamma)$ on $\mathfrak{S}_r^p$ under our identificatio of C_r with $\mathfrak{S}_r^p$. These facts are verified by applying Lemma 1, p. 12-04 o [12] to each factor of $\mathfrak{S}_n \times \cdots \times \mathfrak{S}_n$ and by applying considerations simila to those of pp. 12-14 to 12-15 of [12]. If $\sigma \in Sp(n,\mathfrak{k})^\tau$, we have natura isomorphisms of quotient spaces:

$$\sigma C_r/((\mathfrak{G}_n^r)^{\sigma\tau\rho} \cap \Gamma_{n,p}'^\tau) \cong C_r/((\mathfrak{G}_n^r)^{\tau\rho} \cap \Gamma_{n,p}'^{\sigma^{-1}\tau}) \cong S_r^p/\Gamma_{r,\lambda(\sigma)},$$

where $\Gamma_{r,\lambda(\sigma)}$ is a certain subgroup of $Sp(r,\mathfrak{k})$ commensurable with $\Gamma_{r,p}$ Although $\mathfrak{A}_r^*/\Gamma_{r,\lambda(\sigma)}^\tau$ may be mapped in a continuous, proper manner ont $\operatorname{clos}(C_r)/((\mathfrak{G}_n^r)^{\tau\rho} \cap \Gamma_{n,p}'^{\sigma^{-1}\tau})$, this mapping ψ is not a homeomorphism sinc [12, pp. 13-05 to 13-06] it is not even one-to-one. However, if

$$x \in \operatorname{clos}(C_r)/((\mathfrak{G}_n^r)^{\tau\rho} \cap \Gamma_{n,p}'^{\sigma^{-1}\tau}),$$

$\psi^{-1}(x)$ is a finite set and ψ restricted to $\mathfrak{B}_r^p/\Gamma_{r,\lambda(\sigma)}^\tau$ is actually one-to-one.

The finite number of points in $\mathfrak{B}_{n,0}^*/\Gamma_{n,p}'^\tau$ correspond to the finit number of points in which a true fundamental domain (not just a funda mental open set) meets the distinguished boundary of $\mathfrak{B}_n^p$, and their numbe can be calculated as in [10].

Just as in [12, exposés 12 and 13] it may be proved that $\mathfrak{A}_n^*/\Gamma_{n,p}'^\tau$ i a compact Hausdorff space. It is also easy to see that $\mathfrak{A}_n^*/\Gamma_{n,p}'^\tau$ is the unio of a finite number of pairwise disjoint subspaces isomorphic to comple analytic spaces $\mathfrak{S}_r^p/\Gamma_{r,\lambda}$, $0 \leqq r \leqq n$. We shall now elaborate somewhat on th geometrical situation involved.

As we have just seen, $(\tau\rho)^{-1}$ maps $\mathfrak{B}_n^p$ onto $\mathfrak{S}_n^p$, and may be uniquel extended to a homeomorphism ϕ of $\mathfrak{A}_n^*$ with the union $\mathfrak{S}_n^*$ of a certai

---

[1] It should be noted as a direct consequence of the definition of $Q(t)$ (namel that certain diagonal entries of Y must be of the same order of magnitude) tha $\mathfrak{A}_n^* = \bigcup_r \mathfrak{B}_{n,r}^*$.

countable collection of replicas $\mathfrak{S}_{r,\alpha}{}^p$ of the spaces $\mathfrak{S}_r{}^p$ $(0 \leqq r \leqq n)$ supplied with the finest topology such that each of the injections

$$\gamma\left(\bigcup_{s=0}^{n} \operatorname{clos} \Omega_s\right) \subset \mathfrak{S}_n{}^*, \qquad \gamma \in Sp(n, \mathfrak{k}),$$

is continuous, the action of $\gamma \in Sp(n,\mathfrak{k})$ on $\mathfrak{S}_n{}^*$ being defined in an evident manner. C_r is to be identified with one of the $\mathfrak{S}_{r,\alpha}{}^p$, which we denote simply by $\mathfrak{S}_r{}^p$, and Ω_r is an open subset of $\mathfrak{S}_r{}^p$.

Let $\mathcal{U}$ be an open subset of $\mathfrak{S}_n{}^*$ such that $\Gamma'\mathcal{U} = \mathcal{U}$, and let $\mathcal{U}_r = \mathfrak{S}_r{}^p \cap \mathcal{U}$. It is clear that the closure of $\mathcal{U}_n$ in the topology of $\mathfrak{S}_n{}^*$ contains $\mathcal{U}_r$ for $r < n$. Letting

$$Sp(n,\mathfrak{k}) = \bigcup_{\lambda} \Gamma' M_{r\lambda} \mathfrak{G}_r{}^n$$

be a decomposition of $Sp(n,\mathfrak{k})$ into double cosets mod Γ' and $\mathfrak{G}_r{}^n$ (which, as in [12, exp. 13], may be seen to be finite in number), put

$$\mathcal{U}_{r\lambda} = M_{r\lambda}{}^{-1}\mathcal{U} \cap \mathfrak{S}_r{}^p$$

and

$$\Gamma_{r\lambda} = \pi_r(M_{r\lambda}{}^{-1}\Gamma' M_{r\lambda} \cap \mathfrak{G}_r{}^n).$$

Then $\mathcal{U} = \bigcup_{r,\lambda} \Gamma' M_{r\lambda}\mathcal{U}_{r\lambda}$, and $(\Gamma' M_{r\lambda}\mathcal{U}_{r\lambda}) \cap (\Gamma' M_{s\mu}\mathcal{U}_{s\mu})$ is non-empty only if $r = s$, $\lambda = \mu$. If furthermore $s < r < n$ and

$$Sp(r,k) = \bigcup_{\nu} \Gamma_{r\lambda} M_{s\nu}{}^{r\lambda} \mathfrak{G}_s{}^r,$$

and if $M_{r\lambda}M_{s\nu}{}^{r\lambda} = M' M_{s\mu} L$, $M' \in \Gamma'$, $L \in \mathfrak{G}_s{}^n$, we write $(\lambda,\nu) \to \mu$. It is of course possible that we may have $(\lambda',\nu') \to \mu$, $\lambda' \neq \lambda$, $\nu' \neq \nu$.

The above has the following geometrical significance: A "fundamental open set" [2] $B^*(\Omega)$ for Γ' in $\mathfrak{S}_n{}^*$ consists of the interior of the closure in $\mathfrak{S}_n{}^*$ of the fundamental open set $B'(\Omega)$ for Γ' in $\mathfrak{S}_n{}^p$. For each r, $B^*(\Omega)$ meets a certain finite number of the spaces $\mathfrak{S}_{r,\alpha}{}^p$. Let a maximal subset of these, inequivalent under Γ', be denoted by $\mathfrak{S}_{r\lambda}{}^p$, λ belonging to a finite indexing set Λ, and we may choose the $M_{r\lambda}$ such that $M_{r\lambda}\mathfrak{S}_r{}^p = \mathfrak{S}_{r\lambda}{}^p$. Let $\delta(r) = \frac{1}{2}pr(r+1)$. Then $M_{r\lambda}$ carries the $\delta(r)$-dimensional "vertex" $M_{r\lambda}{}^{-1}B^*(\Omega) \cap \mathfrak{S}_r{}^p$ onto the $\delta(r)$-dimensional vertex $B^*(\Omega) \cap \mathfrak{S}_{r\lambda}{}^p$ of $B^*(\Omega)$. Moreover, $B_{r\lambda}{}^*(\Omega) = M_{r\lambda}{}^{-1}(B^*(\Omega) \cap \mathfrak{S}_{r\lambda}{}^p)$ is a fundamental open set in $\mathfrak{S}_r{}^p$ for the group $\Gamma_{r\lambda}$, and $M_{s\nu}{}^{r\lambda}$ may be chosen to carry the $\delta(s)$-dimensional

[2] Here the use of the term "fundamental open set" is a convenient abuse of language (it is inaccurate because Γ' does not act discontinuously in $\mathfrak{S}_n{}^*$). The term is used here to denote a set containing only a finite number of points from each orbit of Γ' and whose intersection with each of the lower dimensional spaces $\mathfrak{S}_{r,\alpha}{}^p$ is a fundamental open set in this space with respect to a certain group acting there.

vertex $B_{r\lambda}^*(\Omega) \cap \mathfrak{S}_s^p$ onto the $\delta(s)$-dimensional vertex $M_{s\nu}^{r\lambda}(B_{r\lambda}^*(\Omega) \cap \mathfrak{S}_s^p)$ of $B_{r\lambda}^*(\Omega)$, and so $M_{r\lambda}M_{s\nu}^{r\lambda}$ carries the vertex $B_{r\lambda}^*(\Omega) \cap \mathfrak{S}_s^p$ (which is transformed onto some other open domain in $\mathfrak{S}_s^p$ by all $\gamma \in \mathfrak{G}_s^n$) onto some other $\delta(s)$-dimensional space which is a translate under some $M' \in \Gamma'$ of a $\delta(s)$-dimensional vertex contained in, say, $\mathfrak{S}_{s\mu}^p$.

Let $Z_0 \in \Omega_r$, let $\mathfrak{U}_r$ be a connected neighborhood of Z_0, stable under $\pi_r(\Gamma')_{Z_0}$, and let $\mathfrak{U}_s = V^{(s)}(\mathfrak{U}_r, K)$ be defined as before, $r < s \leqq n$, $K > 0$. It is easy to see that there exist a finite number of $M \in (\Gamma^*)_{Z_0}$, say $M_1, \cdots, M_m$, such that the closure of $(\Gamma')_{Z_0}(\bigcup_{i=1}^{m} M_i\mathfrak{U}_n)$ is a (saturated) neighborhood of Z_0 (in $\mathfrak{A}_n^*$, if we identify $\mathfrak{S}_n^p$ with $\mathfrak{B}_n^p$). However, $\bigcup_{1}^{m} M_i\mathfrak{U}_n$ may not be connected. Let $N_1, \cdots, N_k \in Sp(n, \mathfrak{k})_{Z_0}$ be of the form

$$N_j = \begin{pmatrix} {}^tU_j & 0 \\ 0 & U_j^{-1} \end{pmatrix}, \quad \text{where } U_j = \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & e_j \end{bmatrix},$$

and $e_1, \cdots, e_k$ have all possible signatures in $\mathfrak{k}$. Let

$$\left\{ \begin{bmatrix} Z_0^{(l)} & & & 0 \\ & y_{r+1}^{(l)} & & \\ & & \ddots & \\ 0 & & & y_n^{(l)} \end{bmatrix} \right\}_{l=1,\cdots,p} = Z_0^* \in \mathfrak{U}_n.$$

For appropriate *fixed* choice of μ, t, we can always find $y_{r+1}^{(l)}, \cdots, y_n^{(l)}$ (depending on $\mathfrak{U}_n$) such that the "ray" from Z_0^* to Z_0 will be containend in $\mathfrak{U}_n \cap N_j\mathfrak{U}_n$, $j = 1, \cdots, k$. Let G_{Z_0} be the subgroup of $Sp(r, R)^p$ leaving Z_0 fixed. Then the kernel $\mathfrak{N}$ of the canonical homomorphism of $(Sp(n, R)^p)_{Z_0}$ onto G_{Z_0} has as many components as there are different signatures (i.e., 2^p). Therefore if $M_i \in g\mathfrak{N}$, M_i can be joined to one gN_j by a fixed path $\mathcal{K}_i$ in $g\mathfrak{N}$. The union $\mathcal{K} = \bigcup_i \mathcal{K}_i$ is a compact set fxed once for all. Let $\mathcal{L}$ be the (dense) set of points of $iSp(n, \mathfrak{k})$ contained in a fixed compact neighborhood $\mathcal{R}$ of $\mathcal{K}$ in the space consisting of the finite number of cosets $g\mathfrak{N}$ involved. Let $D = (\Gamma')_{Z_0}\mathcal{L}\mathfrak{U}_n$. Since $\mathfrak{U}_r$ is connected, it follows easily from our construction that D is connected. Since each $g \in Sp(n, \mathfrak{k})$ acts continuously on $\mathfrak{A}_n^*$ (with our usual identifications), it is clear that the closure of D is a neighborhood of Z_0. Finally, direct computation shows that, since $\mathcal{R}$ is *compact* and fixed once for all, the closure of D runs over a basis of neighborhoods of Z_0 as $\mathfrak{U}_r$ runs over a basis of connected neighborhoods of Z_0 in $\mathfrak{S}_r$

and $K \to +\infty$. Therefore, since D is connected for each of these, we have (as in [12, pp. 13-08 to 13-10]): *the canonical image of Z_0 in $\mathfrak{S}_n{}^*/\Gamma'$ has a basis of neighborhoods $\{U_\alpha\}$ such that each $U_\alpha \cap (\mathfrak{S}_n{}^p/\Gamma')$ is connected.*

2. Modular forms and Eisenstein series. Let Γ' be a subgroup of $Sp(n, \mathfrak{k})$ commensurable with the modular group $\Gamma = \Gamma_{n,\mathfrak{p}}$. By a (matrix-valued) modular form of weight k and multiplier v with respect to Γ', we mean a holomorphic (matrix-valued) function f on $\mathfrak{S}_n{}^p$ with values in the space $M_q(C)$ of $q \times q$ complex matrices satisfying

$$f(MZ) = N \det(CZ + D)^k f(Z) v(M)^{-1}$$

for $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma'$, where v is a homomorphism of Γ' into $GL(q, C)$ such that the kernel of v is of finite index in Γ'. We denote the module of such forms by $\mathfrak{H}_{n,\Gamma'}(k, v)$, and if $q = 1$ and $v(M) = 1$ for all $M \in \Gamma'$, this module is denoted by $\mathfrak{H}_{n,\Gamma'}(k)$.

Let S be an $n \times n$ symmetric matrix over $\mathfrak{o}$, and assume $S \geqq 0$, which means that each of the conjugates of S is positive semi-definite, all conjugates, of course, being of the same rank r. As in [12] we let

$$\mathfrak{G}_S = \{M \mid M \in \mathfrak{G}_0{}^n,\quad M = \begin{pmatrix} {}^tU & TU^{-1} \\ 0 & U^{-1} \end{pmatrix},\quad US{}^tU = S,\quad \operatorname{tr}(ST) \in \mathfrak{o}\},$$

$$\Gamma_S' = \Gamma' \cap \mathfrak{G}_S.$$

The Eisenstein series $E_{\Gamma';S,k}$ for an even integer k, Γ', and S is defined by

$$E_{\Gamma';S,k}(Z) = \sum_{M:\Gamma_S'\backslash\Gamma'} \epsilon(S \cdot MZ) N \det(CZ + D)^{-k},$$

where $\epsilon(X) = \exp(2\pi i tr(X))$, and where $M : \Gamma_S'\backslash\Gamma'$ means that $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ runs over a complete system of right coset representatives of Γ_S' in Γ'. For fixed k, let $E_{\Gamma';S} = E_{\Gamma';S,k}$.

We shall shortly return to the proof of the convergence of these series for sufficiently large k, noting that is sufficient to prove the convergence of $E_{\Gamma;S}$ because of the following easy propositions:

(I) If Γ'' is a subgroup of Γ', and if $E_{\Gamma';S}$ converges, then $E_{\Gamma'';S}$ converges.

(II) If Γ'' is a normal subgroup of Γ' of finite index, the convergence of $E_{\Gamma'';S}$ implies that of $E_{\Gamma';S}$.

It is easily seen that $E_{\Gamma';S}$ is a modular form of weight k with respect

to Γ'. Moreover, if we define $(f|M)(Z) = f(MZ)N\det(CZ+D)^{-k}$ for any $M \in Sp(n,\mathfrak{k})$, it is clear that

$$E_{M^{-1}\Gamma' M} \mid M \in \mathfrak{H}_{n,\Gamma'}(k).$$

Let $\omega \in GL(q,C)$ be fixed and let

$$\Gamma'_{S,\omega} = \{M \mid M = \begin{pmatrix} {}^tU & TU^{-1} \\ 0 & U^{-1} \end{pmatrix} \in \Gamma' \cap \mathfrak{G}_0{}^n;$$
$$\epsilon(SZ)\omega \mid M = \epsilon(SZ)\omega\},$$

where $\epsilon(SZ)\omega \mid M = \epsilon(SZ)N\det(CZ+D)^k\omega v(M)$ for $M \in Sp(n,\mathfrak{k})$. Then more generally we can consider the series

$$E_{\Gamma';S,\omega}(Z) = \sum_{M:\Gamma'_{S,\omega}\backslash\Gamma'} \epsilon(SZ)\omega|M,$$

which, if it converges, $\in \mathfrak{H}_{n,\Gamma'}(k,v)$. In order to establish the convergence of this it is evidently sufficient to prove the convergence of the series $E_{\Gamma;S}$.

We first consider the case $S \gg 0$. We shall not exhibit many details here because most of these are the same as in [12, exposé 9].

THEOREM 1. *Let S be an $n\times n$ symmetric matrix over $\mathfrak{k}$, $S \gg 0$, and let $E_{\Gamma;S}$ be defined as above. If $k > 2n$, $E_{\Gamma;S}$ converges uniformly on every compact subset of $\mathfrak{S}_n{}^p$.*

Proof. Proceeding as in [12], we let $J(M,Z) = N(\det(CZ+D))^k$, $I(Z) = N(\det Y)^{k/2}$. Then letting $J'(M,Z) = I(MZ)J(M,Z)I(Z)^{-1}$, we see that $|J'(MZ)| = 1$. Therefore if we let $\phi(Z) = I(Z)\epsilon(SZ)$, we have

$$(N(\det Y)^{k/2})E_{\Gamma;S}(Z) = \sum_{M:\Gamma_S\backslash\Gamma} J'(M,z)^{-1}\phi(MZ),$$

and since for holomorphic functions convergence in the $\mathfrak{L}^1$-norm on an open set implies uniform point-wise convergence on every compact subset, it will suffice to prove the convergence of the integral

$$\int_{Z \bmod \Gamma} \sum_{M:\Gamma_S\backslash\Gamma} \|\phi(MZ)\|\, dZ,$$

where $dZ = N((\det Y)^{-n-1}\,dXdY)$ is the invariant measure on $\mathfrak{S}_n{}^p$. This integral is equal to

$$\int_{Z \bmod \Gamma_S} \|\phi(Z)|\, dZ,$$

and since the subgroup Γ_∞ of Γ_S consisting of the translations $M = \begin{pmatrix} E & T \\ 0 & E \end{pmatrix}$

is of finite index in Γ_S (since $US{}^tU = S$ must hold for each of the *conjugates* of U and S), it is therefore sufficient to prove the convergence of

$$\int_{Z \bmod \Gamma_\infty} \| \phi(Z) \| \, dZ$$

$$= \int_{Z \bmod \Gamma_\infty} N(\det Y)^{k/2} \exp(-2\pi tr(SY)) N(\det Y^{-n-1} \, dX dY)$$

$$= \Delta^{n(n+1)/2} \int_{\substack{Y^i >> 0 \\ i=1,\cdots,p}} \prod_i (\det Y^i)^{k/2} \exp(-2\pi \sum_i tr(S^i Y^i)) \prod_i (\det Y^i)^{-n-1} \, dY^i$$

$$= \Delta^{n(n+1)/2} \prod_{i=1}^{p} \int_{Y^i >> 0} (\det Y^i)^{k/2-n-1} \exp(-2\pi tr(S^i Y^i)) \, dY^i,$$

where Δ is the discriminant of $\mathfrak{k}$. Since each of these last factors converges if $k > 2n$, the proof is complete.

Let Γ' be commensurable with Γ. A norm $\| \quad \|_\beta$ is defined on $\mathfrak{H}_{n,\Gamma'}(k)$ by:

$$\| f \|_\beta = \Big(\int_{Z \bmod \Gamma'} | N \det Y^{k/2} \cdot f |^\beta \, dZ \Big)^{1/\beta}.$$

The space of $f \in \mathfrak{H}_{n,\Gamma'}(k)$ with $\| f \|_\beta < +\infty$ is denoted by $\mathfrak{H}_{\Gamma'}{}^{\beta}(k)$. The integral estimate of the preceding proof shows that $E_{\Gamma';S} \in \mathfrak{H}_{\Gamma'}{}^{1}(k)$ if $k > 2n$.

We turn to the proof that $E_{\Gamma,S}$ converges if $S \geqq 0$. This is more difficult than the case $S >> 0$ and we shall give an arithmetic type of proof along the lines of [4, 13], rather than attempt to carry over the proof in [12]. We have

$$E_{\Gamma,S} = \sum_{M : \Gamma_S \backslash \Gamma} \epsilon(S \cdot MZ) N \det(CZ + D)^{-k}.$$

By using the device of [4, p. 391] it is easy to see that we may restrict ourselves to investigating the sum for $\det C \neq 0$. For a fixed symmetric pair (C, D), $\det C \neq 0$, we wish to estimate the sum

$$\phi_{C,D}(Z) = \sum_M \epsilon(S \cdot MZ),$$

where M runs over the same system of coset representatives for the fixed pair (C, D) as in $E_{\Gamma,S}$.

All such representatives can be chosen in the form $\begin{pmatrix} {}^tU & TU^{-1} \\ 0 & U^{-1} \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, A, B being fixed once for all. Then

$$| \phi_{C,D}(Z) | \leqq \sum_U \exp(-2\pi tr(S^i \cdot Y_1{}^i[U^i])),$$

where

$$Y_1 = \operatorname{Im}((A^iZ^i + B^i)(C^iZ^i + D^i)^{-1})$$
$$= {}^t(C^i\bar{Z}^i + D^i)^{-1}Y^i(C^iZ^i + D^i)^{-1} (Y^i = \operatorname{Im} Z^i)$$

and the summation is over a set of coset representatives of the group of units of S in the group of unimodular matrices over $\mathfrak{o}$ (i.e., $\det U$ is a unit of $\mathfrak{o}$). If S is of rank r, this summation is over a certain group of real lattice points in $C^{nr} \times \cdots \times C^{nr} = C^{nrp}$, with appropriate choice of coordinates (these are not products of lattice points in the component factors, but are in correspondence with a certain additive group of $r \times n$ matrices over $\mathfrak{o}$ of finite index I in the group of all such matrices in such a way that the i-th component of the lattice point is the i-th conjugate of the matrix). If

$$V = (V^1, \cdots, V^p) \in C^{nrp},$$

V^i being an $r \times n$ matrix, $(CZ + D)^{-1}$ acts as a linear transformation on C^{nrp} by

$$(CZ + D)^{-1}V = ((C^1Z^1 + D^1)^{-1}V^1, \cdots, (C^pZ^p + D^p)^{-1}V^p),$$

and the *real* determinant (i.e., Jacobian) of this transformation is $|N \det(CZ + D)|^{-2r}$. To estimate $|\phi_{C,D}(Z)|$ for Z belonging to a compact subset of $\mathfrak{S}_n{}^p$, we sum over the lattice points in an expanding sequence of concentric ellipsoidal shells. Namely, if R is the region between two concentric sphere in C^{nrp}, with respect to the metric $tr(\sum_{i=1}^{p} {}^t\bar{V}^iV^i)$, we wish to estimate the number of lattice points of our summation in the ellipsoidal shell which is the image of R under the mapping $(CZ + D)^{-1}$. We have

$$(C^iZ^i + D^i)^{-1}V^i = (Z^i + (C^i)^{-1}D^i)^{-1}(C^i)^{-1}V^i,$$

and $I(\det C^i)(C^i)^{-1}$, having coefficients in $\mathfrak{o}$, is an endomorphism of the set of lattice points, whereas the fact that Z remains in a compact set makes it clear that the ratio of the maximum to the minimum eigenvalue of the transformation $Z + (C)^{-1}D$ is no greater than some constant times $|N \det(Z + (C)^{-1}D)|^{e_1}$, where e_1 is some positive integer. Therefore, the number of lattice points in the ellipsoidal shell is no greater than some constant times $|N(\det(CZ + D))|^{e_1}$, for a suitable (possibly altered) choice of the positive integer e_1. Since

$$|\phi_{C,D}(Z)| \leqq \sum_U \exp(-2\pi tr(S^iY^i[(C^iZ^i + D^i)^{-1}U^i]),$$

it is then clear that

$$\sup_{Z \in K} |\phi_{C,D}(Z)| \leqq C_1 |N \det(CZ + D)|^{e_1},$$

C_1 being a positive constant depending only on the compact set K. Therefore it suffices to prove the convergence of

$$\psi(Z) = \sum_{(C,D),\, \det C \neq 0} |N \det(CZ + D)|^{-(k-e_1)},$$

(C, D) running over a system of left non-associate, symmetric, primitive pairs. We have, letting $k - e_1 = \rho$,

$$\psi(Z) = \sum_{C} |N \det C|^{-\rho} (\sum_{D} |N \det(Z + C^{-1}D)|^{-\rho}).$$

Let $\beta_C(Z) = \sum_{D} |N \det(Z + C^{-1}D)|^{-\rho}$, D running over integral matrices such that (C, D) is symmetric.

We say that two matrices H_1 and H_2 are congruent mod C if $H_1 - H_2 = C \cdot T$, T being integral. It is clear that the number of residue classes mod C of integral D such that $C^{-1}D$ is symmetric is not greater than $|N \det C|^{\frac{1}{2}n(n+1)}$. It is also clear that a representative D_0 from each residue class can be chosen such that $C^{-1}D_0$ lies in a fixed compact subset of the space of real symmetric matrices, independent of C and the particular residue class. Therefore, to prove that $\psi(Z)$ converges uniformly on K, it is sufficient to show that

$$\sum_{C} |N \det C|^{-\rho + \frac{1}{2}n(n+1)} \text{ and } \sum_{H} |N \det(Z + H)|^{-\rho}$$

converge uniformly, where in the second sumation H runs over all symmetric matrices over $\mathfrak{o}$.

If C is a non-singular matrix over $\mathfrak{o}$, the number of left non-associate matrices A over $\mathfrak{o}$ satisfying ${}^tAA = {}^tCC$ is no greater than some constant times $N \det({}^tCC)^{e_2}$ for some positive integer e_2 independent of C. In fact, if ${}^tAA = {}^tCC$, $M = (\det C)(AC^{-1})$ is a matrix over $\mathfrak{o}$ such that ${}^tMM = (\det C)^2 E$, and since, after multiplying C by a suitable unit of $\mathfrak{o}$, we may assume $|(\det C^i)/(\det C^j)| < \lambda$ for all i, j, our assertion follows from a direct computation (here λ is some constant > 1 depending only on the field $\mathfrak{k}$). Since ${}^tCC = S$ is a positive definite matrix with coefficients in $\mathfrak{o}$, we see that

$$\sum_{C} |N \det C|^{-\rho + \frac{1}{2}n(n+1)}$$

converges provided that the following series converges:

$$\sum_{S \gg 0} |N \det(S)|^{-\sigma},$$

where $\sigma = \frac{1}{2}\rho - n(n+1)/4 - e_2$ and where S runs over a system of representatives of equivalence classes of positive definite symmetric matrices over $\mathfrak{o}$

($S_1 \sim S_2$ if there exists a unimodular $n \times n$ matrix U over $\mathfrak{o}$ such that ${}^tUS_1U = S_2$). By Humbert's reduction theory [8], there exists a finite number of matrices $A_1, \cdots, A_m \in GL(n, \mathfrak{k})$ such that for each symmetric $S \gg 0$ there exists μ, $1 \leqq \mu \leqq m$, such that $S[A_\mu]$ is equivalent to a point in the domain $Q(t)$ (q.v., § 1). Therefore the series $\sum_{S \gg 0} | N \det S |^{-\sigma}$ is not greater than $K_1 \cdot \sum_{S \in Q(t)} | N \det S |^{-\sigma}$, K_1 being a positive constant. If $S \in Q(t)$, $S^{(i)} = (s_{jk}^{(i)})$, it is clear that $\det S^{(i)} \geqq C s_{11}^{(i)} \cdots s_{nn}^{(i)}$ and $C \cdot | s_{jk}^{(i)} | \leqq s_{jj}^{(i)}$, all i, j, k, where C is a suitable positive constant and $C s_{jj}^{(i_1)} < s_{jj}^{(i_2)} < C^{-1} s_{jj}^{(i_1)}$ all i_1, i_2, j. Let $N s_{jj} = \tau_j$. For fixed positive rational integers $\tau_1, \cdots, \tau_n$ all the elements in the j-th column of S are such that they, together with all of their conjugates are no greater than $c' \tau_j^{1/p}$. Therefore each of them can take on at most $c'' \tau_j$ values, where c'' depends only on c' and k. Hence, the number of S for given $\tau_1, \cdots, \tau_n$ is at most $c'' \cdot \tau_1 \tau_2^2 \cdot \cdots, \tau_n^n$, and therefore $\sum_{S \in Q(t)} | N \det S |^{-\sigma}$ is majorized by $K' \cdot \sum_{\tau_1, \cdots, \tau_n} \tau_1^{1-\sigma} \cdot \cdots \cdot \tau_n^{n-\sigma}$ which evidently converges if $\sigma > n + 1$.

We now need only show that

$$\sum_H | N \det(Z + H) |^{-\sigma}$$

converges uniformly over every compact for sufficiently large σ. If $Z = X + iY$, we may write (as in [13]) $\mathfrak{P}' Y \mathfrak{P} = E$, $\mathfrak{P}'(X + H)\mathfrak{P} = W$. If $\lambda_1, \cdots, \lambda_n$ are the characteristic roots of W,

$$| \det(Z + H) | = \det Y \cdot \prod_{k=1}^{n} (1 + \lambda_k^2)^{\frac{1}{2}} \geqq \det Y \cdot (1 + \sum_{k=1}^{n} \lambda_k^2)^{\frac{1}{2}}.$$

If we put $\Lambda^2 = \sum_{k=1}^{n} \lambda_k^2$, then $\Lambda^2 = \operatorname{tr}(W^2) = \sum_{i,j} w_{ij}^2$, so that if q is the integer such that $q - 1 \leqq 2\Lambda < q$, we have $| w_{ij} | < q$, all i, j.

$$H = (P')^{-1} W P^{-1} - X$$

and since P and X range over fixed compact sets, this implies the existence of a constant $c > 0$ such that $| h_{ij} | < cq$. Hence, for fixed q, the total number of matrices H such that $q - 1 \leqq (\operatorname{tr}((W^i)^2)) < q$ for each of the conjugates H^i of H is no greater than $c'(q^p)^{\frac{1}{2}n(n+1)}$, and for each such matrix $| N \det(Z + H) | \geqq c'' q$. Therefore, $\sum_H | N \det(Z + H) |^{-\sigma}$ is dominated by $\sum_{q \text{ integral}} q^{-\sigma + \frac{1}{2}pn(n+1)}$ which converges if $\sigma > \frac{1}{2}pn(n+1) + 1$. This is probably (almost certainly) not the best exponent of convergence, but our only aim has been to show the existence of a finite exponent of convergence.

In particular we have shown, in view of (I) and (II), that $\sum_{C,D} | N \det(CZ+D)|^{-\rho}$ converges for sufficiently large ρ, where (C,D) runs over all left non-associate pairs such that some $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma'$. Therefore $\alpha(Z) = [\sum_{C,D} | N \det(CZ+D)|^{-\rho}]^{2/\rho}$ is what Pyateckii-Shapiro [10] calls a normal majorant function for Γ', and according to [10, p. 24 (Lemma 5)] it follows that $\dim H_{n,\Gamma'}(k) < +\infty$.[3]

3. The operator Φ and the ringed structure on $\mathfrak{S}_n^*/\Gamma'$. In this section we shall supply the space $\mathfrak{S}_n^*/\Gamma'$ with a ringed structure, i.e., a subsheaf $\mathfrak{A}$ of the sheaf of germs of continuous, complex-valued functions on $\mathfrak{S}_n^*/\Gamma'$, with respect to which it will be proved later that $\mathfrak{S}_n^*/\Gamma'$ is a normal general analytic space. Because the case $p=1$ has been dealt with in [1, 11, 12], we shall assume here that $p>1$ in order to avoid treatment of special cases.

As usual, Γ' denotes a group commensurable with $\Gamma = \Gamma_{n,p}$. We let Ω, $\mathcal{U}$, $\mathfrak{S}_r^p$, $\mathcal{U}_r$, $M_{r\lambda}$, $\mathfrak{S}_{r\lambda}^p$, $\mathcal{U}_{r\lambda}$, $M_{s\nu}{}^{r\lambda}$, and $\Gamma_{r\lambda}$ have the same meanings as in § 1. Moreover, we let $\mathfrak{B}_{r\lambda} = \mathfrak{S}_{r\lambda}^p / M_{r\lambda}\Gamma_{r\lambda}M_{r\lambda}^{-1}$ and $\mathfrak{B}_n^* = \mathfrak{S}_n^*/\Gamma'$. Then $\mathfrak{B}_n^* = \bigcup_{r,\lambda} \mathfrak{B}_{r\lambda}$.

We denote by $\mathfrak{H}_{n,\Gamma',\mathcal{U}_n}(k,v)$ the module of holomorphic functions on $\mathcal{U}_n$ satisfying

$$f(MZ) = N\det(CZ+D)^k f(Z) v(M)^{-1}, \qquad Z \in \mathcal{U}_n,$$

for $M \in \Gamma'$, k being a non-negative integer and v having its usual meaning. Let $f \in \mathfrak{H}_{n,\Gamma',\mathcal{U}_n}(k,v)$ and let $Z_0 \in \mathcal{U}_r$. By appropriately restricting $\mathcal{U}$, we may asusme that $\mathcal{U}$ is stable under all the *real* translations: $Z \to Z+T$, $Z = (Z^1, \cdots, Z^p)$, $T = (T^1, \cdots, T^p)$, $T^j = \begin{pmatrix} 0 & T_{12}{}^j \\ {}^tT_{12}{}^j & T_2{}^j \end{pmatrix}$, ${}^tT_2{}^j = T_2{}^j$. As in [12, p. 14-02], we have

$$\Gamma' \cap \mathfrak{G}_r{}^n \supset \Gamma'_{Z_0} \supset \Gamma' \cap \mathfrak{N}_r{}^n.$$

Since $\Gamma' \cap \mathfrak{N}_r{}^n$ is commensurable with $\Gamma \cap \mathfrak{N}_r{}^n$, it follows that there exists an integer $q \in \mathfrak{o}$, $q \neq 0$, and a subgroup γ_{n-r}' of finite index in the group of

[3] Since it may not be too easy to establish the bounded convergence of the series for $\alpha(Z)$ in the set $\Omega(\mu,t)$, a normal majorant function may be obtained easily in the following way: By using the fact that the image under $\Phi_{r\lambda}{}^n$ is everywhere dense in $\mathfrak{S}_{r\lambda}$ (a fact which does not make use of the finite dimensionality of the latter) one may establish the existence of a finite number of modular forms $\phi_1, \cdots, \phi_N$ of a suitable high weight having no common zeros on $\mathfrak{S}_n^*$. Then a suitable power of the quantity $|\phi_1|^2 + \cdots + |\phi_N|^2$ provides us with a normal majorant function.

$(n-r)\times(n-r)$ unimodular matrices over $\mathfrak{o}$ such that $\Gamma'\cap\mathfrak{N}_r^n$ contains all of the transformations:

$$\text{(i)}\quad M=\begin{pmatrix} {}^tU & 0\\ 0 & U^{-1}\end{pmatrix},\ U=\begin{pmatrix} E_r & 0\\ 0 & U_2\end{pmatrix},\ U_2\in\gamma_{n-r}'$$

$$\text{(ii)}\quad M=\begin{pmatrix} {}^tU & 0\\ 0 & U^{-1}\end{pmatrix},\ U=\begin{pmatrix} E_r & U_{12}\\ 0 & E_{n-r}\end{pmatrix},\ U_{12}\equiv 0\ (\mathrm{mod}\ q)$$

$$\text{(iii)}\quad M=\begin{pmatrix} E & T\\ 0 & E\end{pmatrix},\ T=\begin{pmatrix} 0 & T_{12}\\ {}^tT_{12} & T_2\end{pmatrix},\ T_2={}^tT_2,$$
$$T_{12}, T_2\equiv 0\ (\mathrm{mod}\ q)$$

where we may suppose v to be trivial on M in (i), (ii), and (iii). Therefore f has a Fourier expansion in the connected component of $\mathfrak{U}_n$ to the closure of which belongs Z_0:

$$\begin{aligned} f(Z) &= \textstyle\sum_{S_2} a_{S_2}(Z_1, Z_{12})\,\epsilon(S_2Z_2)\\ &= \textstyle\sum_{S_2,S_{12}} b_{S_2,S_{12}}(Z_1)\,\epsilon({}^tS_{12}Z_{12}+S_2Z_2)\end{aligned}$$

the summation being over matrices S_2, S_{12} with entries in $\mathfrak{k}$ such that $\mathrm{tr}(S_2T_2)$, $\mathrm{tr}({}^tS_{12}T_{12})$ are integral if T is as in (iii). These series converge uniformly on every compact subset of $\mathfrak{U}_n$.

From the uniqueness of the Fourier expansions and from the fact that f must be invariant under a subgroup of finite index in $\Gamma'\cap\mathfrak{N}_r^n$, we see as in [12] that the coefficients a_{S_2} and $b_{S_2,S_{12}}$ must satisfy the following:

(a) $a_{S_2[{}^tU_2]}(Z_1, Z_{12}) = \det U^k a_{S_2}(Z_1, Z_{12}U_2)$,

(b) $a_{S_2}(Z_1, Z_{12}+Z_1U_{12}) = \det U^{-k} a_{S_2}(Z_1, Z_{12})$
$\cdot\,\epsilon(-S_2(Z_1[U_{12}]+2\,{}^tU_{12}Z_{12}))$

(c) $a_{S_2}(Z_1, Z_{12}+T_{12}) = a_{S_2}(Z_1, Z_{12})$

(d) $b_{S_2[{}^tU_2],S_{12}{}^tU_{12}}(Z_1) = \det U^k b_{S_2,S_{12}}(Z_1)$

(e) $b_{S_2,S_{12}+2U_{12}S_2}(Z_1) = \det U^k b_{S_2,S_{12}}(Z_1)\,\epsilon(S_2Z_1[U_{12}]+{}^tS_{12}Z_1U_{12})$

for all M in (i), (ii), (iii). We say that S_{12} is rational multiple of S_2 if there exists an $r\times(n-r)$ matrix W over $\mathfrak{k}$ such that $S_{12}=WS$. It is seen just as in [12] that if $n\geqq 2$, $b_{S_2,S_{12}}(Z_1)\neq 0$ implies that S_{12} is a rational multiple of S_2. If $r>0$, we have from (d) (putting $U_{12}=qU_{12}'$):

$$\begin{aligned} &a_{S_2}(Z_1, Z_{12})\\ &\quad=\sum_{S_{12}\,\mathrm{mod}\,\{2qU_{12}'S_2\}}\ \sum_{U'_{12}\,\mathrm{mod}\,U(S_2)} b_{S_2,S_{12}+2qU_{12}'S_2}(Z_1)\,\epsilon({}^tS_{12}Z_{12}+2qS_2{}^tU_{12}'Z_{12})\\ &\quad=\sum_{S_{12}}\sum_{U_{12}'} \det U^k b_{S_2,S_{12}}(Z_1)\,\epsilon(q^2S_2Z_1[U_1{}'_2]+q\,{}^tS_{12}Z_1U_{12}'\\ &\qquad\qquad +2qS_2{}^tU_{12}'Z_{12}+{}^tS_{12}Z_2),\end{aligned}$$

$U(S_2)$ denoting the set of U_{12}' such that $U_{12}'S_2 = 0$. The series

$$\sum_{U_{12}'} |\epsilon(q^2 S_2 Z_1[U_{12}'] + q({}^tS_{12}Z_1 + 2S_2{}^tZ_{12})U_{12}')|$$

must therefore converge. There exists a non-singular matrix P over $\mathfrak{k}$ such that $S_2 = P\begin{pmatrix} S_2{}^0 & 0 \\ 0 & 0 \end{pmatrix}{}^tP$, $S_{12} = (S_{12}{}^0 0)\,{}^tP$, where $S_2{}^0$ is a non-singular matrix of rank $t \leqq n - r$ and $S_{12}{}^0$ is $r \times t$. Then the convergence of the above series of absolute values implies that of the following series:

$$\sum_{U_{12}''} |\epsilon((q_1)^2 S_2{}^0 Z_1[U_{12}''] + q_1({}^tS_{12}{}^0 Z_1 + 2S_2{}^0{}^tZ_{12}{}^0)U_{12}''|,$$

the summation being taken over all $r \times t$ matrices over $\mathfrak{o}$. Choosing $U_{12}'' = (g\,0\cdots 0)$, where g is any $(n-r)$-(column) vector in $\mathfrak{o}^t$, we see that

$$\sum_g \exp(-2\pi(\sum_\rho [(q_1{}^{(\rho)})^2 y_{11}{}^{(\rho)}(S_2{}^0)^{(\rho)}[g^{(\rho)}] + {}^tb^{(\rho)}g^{(\rho)}]))$$

must converge, where b depends on $S_{12}{}^0$, $S_2{}^0$, Z_1, $Z_{12}{}^0$, the summation on ρ being over the distinct isomorphisms of $\mathfrak{k}$ into R. Suppose $S_2{}^0$ is not positive definite. Choose g such that $(S_2{}^0)^{(\sigma)}[g^{(\sigma)}] < 0$ and let e be a unit in $\mathfrak{k}$ such that $|e^{(\sigma)}| > 1$, $|e^{(\rho)}| < 1$ if $\rho \neq \sigma$. Then

$$\sum_m \exp(-2\pi(\sum_{\rho\neq\sigma} y_{11}{}^{(\rho)} e^{(\rho)2m}(S_2{}^0)^{(\rho)}[g^{(\rho)}] + y_{11}{}^{(\sigma)}e^{(\sigma)2m}(S_2{}^0)^{(\sigma)}[g^{(\sigma)}] + \sum_\rho {}^tb^{(\rho)}g^{(\rho)}(e^{(\rho)2m}))$$

must converge, being a subseries of the above — but this is evidently impossible. Hence $S_2{}^0 \gg 0$.

If $r = 0$, we have the following from (a)

$$a_{S_2[{}^tU_2]} = \det U^k a_{S_2} \tag{1}$$

as well as the estimate

$$|a_{S_2}| \leqq K \exp(\operatorname{tr} S_2) \tag{2}$$

derived from the convergence of the Fourier series $\sum a_{S_2}\epsilon(S_2Z_2)$. From (1) and (2) we easily deduce

$$|a_{S_2}| \leqq K\,|\det U^k|\exp(\operatorname{tr}({}^tUS_2U)) \tag{3}$$

for any $n \times n$ unimodular $U \equiv E \pmod q$. If $n \geqq 2$, and if $S_2{}^{(\sigma)}$ is indefinite, we can "isolate" the terms $\operatorname{tr}({}^tU^{(\sigma)}S_2{}^{(\sigma)}U^{(\sigma)})$ by finding a unit $e \equiv 1 \pmod{N(q)}$ such that $|e^{(\rho)}| < 1$ if $\rho \neq \sigma$, $|e^{(\sigma)}| > 1$, and then multiplying U by e^m for sufficiently large m. Then by Koecher's argument [12 exp. 4] it follows that

$a_{S_2} = 0$. If $n = 1$, $\operatorname{tr}({}^tUS_2U) = \sum_\rho s^{(\rho)}(u^{(\rho)})^2$. Supposing $s^{(\sigma)} < 0$, we could choose e as before and let $u^{(\sigma)} = (e^{(\sigma)})^m$. Using (3) and letting $m \to \infty$ we easily deduce that $a_S = 0$ (this is the same argument as in [6]). Therefore, if $p > 1$, the restriction $n > 1$ is unnecessary in order to guarantee that $a_{S_2} \neq 0$ only if $S_2 \geqq 0$.

Since $a_0(Z_1, Z_{12}) = b_{00}(Z_1)$ depends only on Z_1 and is a holomorphic function in a neighborhood of Z_0, we may define $f_r(Z_1) = (\Phi_r{}^n f)(Z_1) = b_{00}(Z_1)$. Then it may be verified as in [12, pp. 14-08 to 14-10] that $f_r \in \mathfrak{H}_{n,\Gamma_r{}',U_r}(k, v_r)$, where $\Gamma_r{}' = \pi_r(\Gamma' \cap \mathfrak{G}_r{}^n)$ and $v_r(M_1) = \det D_2{}^{-k} v(M)$ acts naturally on a certain quotient space of C^q $(v(M) \in GL(q, C))$ which, for our purposes, is unnecessary to specify (here

$$M = \begin{pmatrix} A_1 & 0 & B_1 & B_{12} \\ A_{21} & A_2 & B_{21} & B_2 \\ C_1 & 0 & D_1 & D_{12} \\ 0 & 0 & 0 & D_2 \end{pmatrix} \in \Gamma' \cap \mathfrak{G}_r{}^n \cap \pi_r{}^{-1}(M_1)).$$

Moreover, it is not hard to verify that $\lim_{Z_\nu \to Z_0} f(Z_\nu) = f_r(Z_0)$ for any sequence $\{Z_\nu\} \subset \mathfrak{U}_n$ converging to Z_0. Finally, if $s < r < n$, it may be verified without difficulty that $\Phi_s{}^r \Phi_r{}^n = \Phi_s{}^n$.

Let $M \in Sp(n, \mathfrak{k})$. Then as in [12, p. 14-13], $f \mid M \in \mathfrak{H}_{M^{-1}\Gamma' M, M^{-1}\mathfrak{U}_n}(k, v_M)$, where $v_M(M^{-1}M'M) = v(M')$, so that

$$\Phi_r{}^n(f \mid M) \in \mathfrak{H}_{\pi_r(M^{-1}\Gamma' M \cap \mathfrak{G}_r{}^n), M^{-1}\mathfrak{U} \cap \mathfrak{S}_r{}^p}(k, v_{Mr}).$$

If, furthermore, $L \in \mathfrak{G}_r{}^n$, it can easily be shown that $\Phi_r{}^n(f \mid ML) = \Phi_r{}^n(f \mid M) \mid \pi_r(L)$. We define

$$f_{r\lambda} = \Phi_{r\lambda}{}^n f = \Phi_r{}^n(f \mid M_{r\lambda}),$$

for $f \in \mathfrak{H}_{n,\Gamma',\mathfrak{U}_n}(k, v)$, so that

$$f_{r\lambda} \in \mathfrak{H}_{r,\Gamma_{r\lambda}, \mathfrak{U}_{r\lambda}}(k, v_{r\lambda}).$$

If furthermore $s < r < n$ and if $(\lambda, \nu) \to \mu$, then

$$\Phi_{s\nu}{}^{r\lambda} \Phi_{r\lambda}{}^n f = \Phi_{s\mu}{}^n f \mid \pi_s(L)$$

if $M_{r\lambda} M_{s\nu}{}^{r\lambda} = M' M_{s\mu} L$, $M' \in \Gamma'$, $L \in \mathfrak{G}_s{}^n$. The proofs of the above, being purely formal, are in no way different from those in [12]. By means of the correspondence: $f \to f \circ M_{r\lambda}{}^{-1}$, the module $\mathfrak{H}_{r,\Gamma_{r\lambda}, \ r\lambda}(k, v_{r\lambda})$ can then be identified with $\mathfrak{H}_{r,M_{r\lambda}\Gamma_{r\lambda}M_{r\lambda}{}^{-1}, M_{r\lambda}U_{r\lambda}}(k, v_{r\lambda}{}^*)$, where $v_{r\lambda}{}^*(M_{r\lambda} M_r M_{r\lambda}{}^{-1}) = v_{r\lambda}(M_r)$, $M_r \in \Gamma_{r\lambda}$. In particular, $\mathfrak{H}_{r,\Gamma_{r\lambda}}(k)$ may be identified with $\mathfrak{H}_{r,M_{r\lambda}\Gamma_{r\lambda}M_{r\lambda}{}^{-1}}(k)$.

For fixed r, λ, let $\mathfrak{S}_{r\lambda}(k, v_{r\lambda})$ denote the intersection (in $\mathfrak{H}_{r,\Gamma_{r\lambda}}(k, v_{r\lambda})$) of the kernels of all the maps $\Phi_{s\nu}{}^{r\lambda}$. $\mathfrak{S}_{r\lambda}(k, v_{r\lambda})$ is known as the module of cusp forms. Let

$$\mathfrak{H}_r(k) = \prod_\lambda \mathfrak{H}_{r,\Gamma_{r\lambda}}(k, v_{r\lambda}), \qquad \mathfrak{S}_r(k) = \prod_\lambda \mathfrak{S}_{r\lambda}(k, v_{r\lambda}),$$

and in particular let $\mathfrak{H}_{0\lambda}(k) = \mathfrak{S}_{0\lambda}(k) = C$ for all λ. It is clear that the homomorphisms $\Phi_{r\lambda}{}^n$ taken together give a single homomorphism

$$\Phi_{(r)}{}^n \colon \mathfrak{H}_n(k) \to \mathfrak{H}_r(k).$$

In general, $\Phi_{(r)}{}^n$ is not onto, but, as we shall see, $\mathfrak{S}_r(k)$ is contained in the image of $\Phi_{(r)}{}^n$.

If $f \in \mathfrak{H}_{n,\Gamma',\mathfrak{U}_n}(k)$, we consider the collection $(f_{r\lambda})$, $f_{r\lambda} = \Phi_{r\lambda}{}^n f$, all r, λ. Such a collection is called a modular form of weight k on $\mathfrak{U}$. By virtue of the mappings $M_{r\lambda}$, a modular form ϕ of weight k on $\mathfrak{U}$ gives rise to a modular form of weight k with respect to $M_{r\lambda}\Gamma_{r\lambda}M_{r\lambda}{}^{-1}$ on $M_{r\lambda}U_{r\lambda} \subset \mathfrak{S}_{r\lambda}{}^p$. Because of the continuity of the mapping Φ (i. e., $\lim_{Z_\nu \to Z_0} f(Z_\nu) = f_r(Z_0)$), it is easily seen that there is a certain complex line bundle $F(k)$ over $\mathfrak{V}_n{}^*$ such that the modular forms of weight k on $\mathfrak{U}$ in a natural manner represent continuous cross-sections of $F(k)$ over the natural image of $\mathfrak{U}$ in $\mathfrak{V}_n{}^*$, and that $F(k)$ is uniquely defined by this requirement.

If $f \in \mathfrak{H}_{n,\Gamma'}(k, v)$, f is invariant under a group $\mathfrak{T}$ of translations: $Z \to Z + T$ of finite index in the group $\Gamma_\infty{}'$ of all translations in Γ'. Therefore it is easily seen that f has a Fourier expansion

$$f(Z) = \sum a_S \epsilon(SZ), \qquad a_S \in M_q(C),$$

where the summation is extended over all S such that $\operatorname{tr}(ST)$ is an integer for all $T \in \mathfrak{T}$. If we define $(f \mid M)(Z) = N \det(CZ + D)^{-k} f(MZ)$ for $M \in Sp(n, \mathfrak{k})$, it is not hard to show that $f \mid M \in \mathfrak{H}_{n,M^{-1}\Gamma' M}(k, v_M)$, where $v_M(M^{-1}M'M) = v(M')$. $(f \mid M)$ also has a Fourier expansion $(f \mid M)(Z) = \sum a_{S_M} \epsilon(S_M Z)$. If for each M it is true that $a_{S_M} \neq 0$ implies $S_M \geqq 0$, f is called integral. If for each M it is true that $a_{S_M} \neq 0$ implies $S_M \gg 0$, f is clearly a cusp form (by the continuity of the operator Φ). We have seen that $p > 1$ or $n > 1$ implies that every modular form is an integral form. Satake has proved [12], in the case $p = 1$, that if $\beta k \geqq 2n$, then $\mathfrak{S}_n(k) = \mathfrak{H}_{n,\Gamma'}{}^\beta(k)$. In our case $(p > 1)$, the proof that $\mathfrak{S}_n(k) \subset \mathfrak{H}_{n,\Gamma'}{}^\beta(k)$ is exactly as on p. 7-09 of [12], because in order to show that a given $f \in \mathfrak{H}_{n,\Gamma'}(k)$ belongs to $\mathfrak{H}_{n,\Gamma'}{}^\beta(k)$, it is sufficient to show, since Ω has finite (invariant) volume, that $(f \mid M_{n-1\lambda})$ approaches zero exponentially as $y_{nn}{}^i$ approach $+\infty$ in the domain Ω for each λ; and this condition is evidently satisfied for the cusp forms (and

not merely for those such that $a_{S_M} \neq 0$ implies $S_M \gg 0$; we can see this by applying the more or less obvious generalizations of Lemmas VII and VIII of [1] for $Y \in \Omega$ and observing that as a result of these the Fourier series for $f \mid M$ can be written as the sum of a finite number of terms, each of which is $\mathcal{O}(e^{-cy_{nn}{}^t})$ for some $c > 0$. However, inasmuch as consideration of only the forms for which $a_{S_M} \neq 0$ implies $S_M \gg 0$ is sufficient for our purposes, we do not dwell on the details here, and only remark the above for the sake of completeness. As a matter of fact, though, we shall shortly see that the latter type of cusp form is the *only* type of cusp form.) In case $k\beta \geqq 2(n+1)$, it can be proved that $\mathfrak{H}_{n,\Gamma'}{}^{\beta}(k) \subset \mathcal{S}_n(k)$, in a manner analogous to that on pp. 9-33 to 9-35 of [12] by considering each of the finitely many $\delta(n-1)$-dimensional vertices of $B'(\Omega)$ in turn, noting that $M^{-1}\Gamma' M \cap \mathfrak{G}_n{}^{n-1}$ is commensurable with $\Gamma \cap \mathfrak{G}_n{}^{n-1}$ for $M \in Sp(n, \mathfrak{k})$. In fact, using the same line of reasoning as on pp. 9-33 to 9-35 of [12] it is not hard to see that if $Z_1 \in \mathfrak{S}_{n-1}{}^p$, $(\Phi_{n-1}{}^n f)(Z_1) \neq 0$, and if $V^{(n)}(\mathcal{U}_{n-1}, K)$ is a suitably small neighborhood of Z_1 in $\mathfrak{S}_n{}^*$, then

$$\int_{V^{(n)}(\mathcal{U}_{n-1}, K)} \| N \det(Y)^{k/2} f(Z) \|^{\beta} \, dZ$$

is bounded from below by

$$c \cdot \int_K^{\infty} \int_K^{t d_n{}^{(p)}} \cdots \int_K^{t d_n{}^{(2)}} (d_n{}^{(1)} \cdots d_n{}^{(p)})^{\frac{1}{2}k\beta - n - 1} \, dd_n{}^{(1)} \cdots dd_n{}^{(p)}$$

$$\geqq c' \int_K^{\infty} (d_n{}^{(p)})^{p(\frac{1}{2}k\beta - n - 1) + p - 1} \, dd_n{}^{(p)}$$

$(c, c' > 0)$ which diverges if $p(\frac{1}{2}k\beta - n - 1) + p \geqq 0$, i.e., if $\frac{1}{2}k\beta \geqq n$ or $k\beta \geqq 2n$. This characterization of the cusp forms makes it clear that if $f \in \mathcal{S}_{n,\Gamma'}(k)$ and if $M \in Sp(n, \mathfrak{k})$, then $(f \mid M) \in \mathcal{S}_n(k)$, because if $| N \det Y |^{k\beta/2} | f(Z) |^{\beta}$ is integrable over $B'(\Omega)$, then $| N \det Y |^{k\beta/2} | (f \mid M) |^{\beta}$ is integrable over $M^{-1}B'(\Omega)$ which is a fundamental open set for $M^{-1}\Gamma' M$. On the other hand, if the Fourier expansion of f contains the term $a \cdot \epsilon(SZ)$, $a \neq 0$, that of $f \mid M$ contains the term $ca \cdot \epsilon(S[{}^tU]Z)$ if $M = \begin{pmatrix} {}^tU & 0 \\ 0 & U^{-1} \end{pmatrix}$, where $c = N(\det U)^{-k}$, and by appropriate choice of U we may assume $S[{}^tU] = \begin{pmatrix} S^* & 0 \\ 0 & 0 \end{pmatrix}$, where $S^* \gg 0$ has the same rank as S. If rank $S^* < n$, it is clear that $\Phi_{n-1}{}^n(f \mid M) \neq 0$, which is a contradiction. Hence the cusp forms f are just those such that if $f \mid M = \sum a_{S_M} \epsilon(S_M Z)$, $M \in Sp(n, \mathfrak{k})$, then $a_{S_M} \neq 0$ implies $S_M \gg 0$. Finally we observe that for $S \gg 0$ we have $E_{\Gamma'; S} \in \mathfrak{H}_{\Gamma'}{}^1(k) = \mathcal{S}_n(k)$ if k is sufficiently large.

As we have seen, the modular forms of a given type form a finite dimensional vector space over C, and in particular the cusp forms are a (finite-dimensional) subspace of this. If as in [12] we define

$$H_k(S)=\int_{Y>>0} N\det Y^k \exp(-\pi\mathrm{tr}(SY))N\det Y^{-n-1}\,dY$$
$$=\int_{Y>>0} N\det Y^{k-n-1}\exp(-\pi\mathrm{tr}(SY))\,dY,$$

we may verify by the same steps as in [12, pp. 9-08 to 9-09] or [9, pp. 574-5] that if $f\in\mathfrak{S}_n(k,v)$ and if $S>>0$, ω given, then

$$\langle f,E_{S;\omega}\rangle=c\cdot\mathrm{tr}[\omega^*H_k(4S)\hat{f}(S)],\tag{4}$$

$*$ denoting conjugate transpose, c a constant depending on $\mathfrak{k}$ and S and $\hat{f}(S)$ the coefficient of $\epsilon(SZ)$ in the Fourier expansion of f, and where $\langle f,g\rangle$ is defined for $f,g\in\mathfrak{H}_{n,\Gamma'}{}^2(k,v)$ by

$$\langle f,g\rangle=\int_{Z \bmod \Gamma}\mathrm{tr}(g(Z)^*N\det Y^k f(Z))\,dZ,\tag{5}$$

dZ being the $Sp(n,\mathfrak{k})$-invariant measure on $\mathfrak{S}_n{}^p$.

In view of (4) it is clear that the Eisenstein series $E_{S;\omega}$ span the space of cusp forms for Γ. By the use of the same "cutting down" and "averaging" processes as on pp. 16-08 to 16-11 of [12], it is not difficult to see that this result may be generalized from Γ to Γ' and that $\mathcal{S}_{n,\Gamma'}(k,v)$ is spanned by the transforms of the Eisenstein series $E_{\Gamma';S,\omega}$, $S>>0$, by $M\in Sp(n,\mathfrak{k})$ (i.e., by the sedies $E_{M^{-1}\Gamma'M;S,\omega}\,|\,M^{-1}$, $S>>0$, $M\in Sp(n,\mathfrak{k})$).

4. Global ontoness of Φ. We refer here to the notation of § 3 and the approach of [12, pp. 16-01 ff.]. Our aim is to show for each r, $0\leqq r\leqq n-1$, that $\mathcal{S}_r(k)\subset\Phi_{(r)}{}^n(\mathfrak{H}_n(k))$. For this it is clearly sufficient to show that if $f_{r\lambda}\in\mathcal{S}_{r\lambda}(k)$, then there exists $f\in\mathfrak{H}_n(k)$ such that $\Phi_{r\lambda}{}^nf=f_{r\lambda}$, $\Phi_{r\lambda'}{}^nf=0$ if $\lambda'\neq\lambda$. Since $\mathcal{S}_{r\lambda}(k)$ is generated by the transforms of the series $E_{\Gamma_{r\lambda}';S_r}$, $S_r>>0$, it follows that it is sufficient to establish for each $S_r>>0$ and $L_1\in Sp(r,\mathfrak{k})$ the existence of $f\in\mathfrak{H}_n(k)$ such that

$$\Phi_{(r)}{}^nf=(0,\cdots,0,E_{L_1\Gamma_{r\lambda}'L_1^{-1};S_r}\,|\,L_1,0,\cdots,0).$$

We shall prove this by computing $\Phi_{(r)}{}^n(E_{M_0^{-1}\Gamma'M_0;S}\,|\,M_0^{-1})$, $M_0\in Sp(n,\mathfrak{k})$. If

$$M_0=\begin{pmatrix}{}^tU_0 & T_0U_0^{-1}\\ 0 & U_0^{-1}\end{pmatrix}\in\mathfrak{G}_0{}^n,\qquad E_{M_0\Gamma'M_0^{-1};S}\,|\,M_0=(\det U_0)^k\epsilon(ST_0)E_{\Gamma';U_0S{}^tU_0}.$$

Therefore, we may assume $S=\begin{pmatrix}S_0 & 0\\ 0 & 0\end{pmatrix}$, $S_0>>0$ of rank t.

Because the class number of $\mathfrak{k}$ is in general >1, we cannot in general say that every element M of $\Gamma_{n,p}$ can be written in the form

$$M=\begin{pmatrix} {}^tU & TU^{-1} \\ 0 & U^{-1} \end{pmatrix}\begin{bmatrix} A_0 & 0 & B_0 & 0 \\ 0 & E & 0 & 0 \\ C_0 & 0 & D_0 & 0 \\ 0 & 0 & 0 & E \end{bmatrix}\begin{pmatrix} {}^tV & 0 \\ 0 & V^{-1} \end{pmatrix},$$

where $\begin{pmatrix} A_0 & B_0 \\ C_0 & D_0 \end{pmatrix} \in \Gamma_{s,p}$, $\det C_0 \neq 0$, ${}^tT=T$ has coefficients in $\mathfrak{o}$, and U, V belong to the group of $n\times n$ unimodular matrices over $\mathfrak{o}$ (as is the case, according to Siegel [14], if the class number of $\mathfrak{k}$ is 1). However, every $M\in Sp(n,\mathfrak{k})$ can be written in the above form if we require only that $U, V\in GL(n,\mathfrak{k})$, and $\begin{pmatrix} A_0 & B_0 \\ C_0 & D_0 \end{pmatrix}\in Sp(s,\mathfrak{k})$, $\det C_0\neq 0$. Let $Z_0\in\mathfrak{S}_r^p$. We now wish to compute $\lim\limits_{Z\to Z_0}\epsilon(SZ)\,|M$, $S=\begin{pmatrix} S_0 & 0 \\ 0 & 0 \end{pmatrix}$, $S_0>>0$ of rank t, $M\in Sp(n,\mathfrak{k})$. If $M=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in Sp(n,\mathfrak{k})$ is written in the above form, we have

$$\begin{aligned} |N\det U|\,|N\det(CZ+D)| &= |N\det C_0|\,|N\det(Z[Q]+C_0^{-1}D_0)| \\ &\geqq |N\det C_0|\,N\det Y[Q], \end{aligned}$$

where Q is the $n\times s$ matrix made up of the first s-columns of V. By replacing V by VU^*A_μ, where A_μ is one of a *finite* number of matrices in $GL(n,\mathfrak{k})$ and U^* is unimodular, $A_\mu=\begin{pmatrix} A_\mu' & 0 \\ 0 & E \end{pmatrix}$, $U^*=\begin{pmatrix} U^{*\prime} & 0 \\ 0 & E \end{pmatrix}$, we may assume $Y[Q]\in Q(t)$ and since the fixed C_0 is then replaced by $C_0{}^tA_\mu'^{-1}U^{*\prime-1}$, we may assume that $|N\det C_0|\geqq c_1$. If $Y[Q]\in Q(t)$,

$$|N\det Y[Q]|\geqq c_2\prod_{i=1}^{s}\prod_{j=1}^{p}Y^j[q_i^j],$$

where c_2 is a constant (depending only on n and s) and where q_i are the columns of Q. Therefore

$$\lim_{Z\to Z_0}\epsilon(SZ)\,|M=\lim_{Z\to Z_0}\epsilon(S\cdot MZ)N\det(CZ+D)^{-k}=0$$

unless $Q=\begin{pmatrix} Q_1 \\ 0 \end{pmatrix}$, Q_1 being $r\times s$, $s\leqq r$. In the latter case we may assume

$$V=\begin{pmatrix} V_1 & 0 \\ 0 & E \end{pmatrix},$$

V_1 being $r\times r$. Proceeding further as in [12, pp. 16-13 to 16-14] we deduce

further that $\lim\limits_{Z\to Z_0} \epsilon(SZ)\,|\,M=0$ unless the matrix P composed of the first r columns of U is of the form

$$P=\begin{pmatrix} P_1 \\ 0 \end{pmatrix}$$

P_1 being $r\times r$, and finally unless $M=NL$, $N\in\mathfrak{G}_S$, $L\in\mathfrak{G}_r{}^n$, so that if

$$L=\begin{bmatrix} A_1 & 0 & B_1 & * \\ * & A_2 & * & * \\ C_1 & 0 & D_1 & * \\ 0 & 0 & 0 & D_2 \end{bmatrix},\ L_1=\pi(L)=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}\in Sp(r,\mathfrak{k}),$$

we have $\lim\limits_{Z\to Z_0} \epsilon(SZ)\,|\,M=N(\det U)^{-k}N(\det D_2)^{-k}\epsilon(S_0Z_0)\,|\,L_1$. For given M, it is clear that $(\det U)(\det D_2)^{-1}$ depends only on L_1.

Then if we wish to calculate

$$\Phi_{r\lambda}{}^n(E_{M_0^{-1}\Gamma' M_0;S}\,|\,M_0{}^{-1})=\Phi_r{}^n(E_{M_0^{-1}\Gamma' M_0;S}\,|\,M_0{}^{-1}M_{r\lambda}),$$

it is evidently sufficient to calculate

$$\Phi_r{}^n(E_{\Gamma'';S}\,|\,M_1)(Z_0)=\lim_{Z\to Z_0}\sum_{M:\,\Gamma_S''\backslash\Gamma''M_1}\epsilon(SZ)\,|\,M,$$

where we may suppose that Z remains in the union of a finite number of translates of Ω under elements of $Sp(n,\mathfrak{k})$. Since the calculations are purely formal in nature, apart from establishing the region of uniform convergence of a simple Eisenstein series in one variable, we omit these with the remark that the computations are just as in [12, pp. 16-04 to 16-06 and pp. 16-15 to 16-16; on line 6 from the top of p. 16-16, $C_{M_1}=0$ should be $C_{M_1}\neq 0$] and write down the final result that if $S=\begin{pmatrix} S_0 & 0 \\ 0 & 0 \end{pmatrix}$, where $S_0\gg 0$, rank $S_0=r$, then

$$\Phi_r{}^n(E_{\Gamma'';S}\,|\,M_1)=\begin{cases} cE_{\pi_r(\Gamma''\cap\mathfrak{G}_r{}^n);S_0}\,|\,L_1 \text{ if } \Gamma''M_1\cap\mathfrak{G}_r{}^n\neq\emptyset, \\ (L\in\Gamma''M_1\cap\mathfrak{G}_r{}^n,\ L_1=\pi_r(L)), \\ 0 \text{ otherwise,} \end{cases}$$

where $c\neq 0$.

Therefore, letting $\Gamma''=M_0{}^{-1}\Gamma' M_0$, $M_1=M_0{}^{-1}M_{r\lambda}$,

$$\Phi_{r\lambda}{}^n(E_{M_0^{-1}\Gamma' M_0;S}\,|\,M_0{}^{-1})=\begin{cases} cE_{L_1\Gamma_{r\lambda}L_1^{-1};S_0}\,|\,L_1 \text{ if } M_0\in\Gamma' M_{r\lambda}\mathfrak{G}_r{}^n, \\ (L\in M_0{}^{-1}\Gamma' M_{r\lambda}\cap\mathfrak{G}_r{}^n,\ L_1=\pi_r(L),\ c\neq 0), \\ 0 \text{ otherwise.} \end{cases}$$

Since, as remarked, the space of cusp form for $\Gamma_{r\lambda}'$ is generated by the transforms $E_{L_1\Gamma_{r\lambda}L_1^{-1};S_0}\,|\,L_1$ of the series $E_{\Gamma_{r\lambda}';S_0}$, $S_0\gg 0$, we see that $\mathcal{S}_r\subset\Phi_{(r)}{}^n\mathfrak{H}_n$.

5. The analytic structure on $\mathfrak{S}_n^*/\Gamma_{n,p}'$. The compactified space $\mathfrak{S}_n^*/\Gamma_{n,p}'$ can be written as a union:

$$\mathfrak{V}_n^* = \mathfrak{S}_n^*/\Gamma_{n,p}' = \bigcup_r \bigcup_\lambda (\mathfrak{S}_r^p)/\Gamma_{r\lambda,p}' = \bigcup_{r,\lambda} V_{r\lambda}.$$

$V_n = \mathfrak{S}_n^p/\Gamma_{n,p}'$ is everywhere dense in this space, and for each r, λ, $V_{r\lambda} = (\mathfrak{S}_r^p)/\Gamma_{r\lambda,p}'$ is a general analytic space of dimension $\frac{1}{2}pr(r+1)$. If $\mathcal{O}$ is an open subset of $\mathfrak{S}_n^*/\Gamma_{n,p}'$ and f a complex-valued continuous function on $\mathcal{O}$, we say that f is an $\mathfrak{A}$-function on $\mathcal{O}$ if $f\,|\,(\mathfrak{V}_n \cap \mathcal{O})$ is analytic in the natural analytic structure on $\mathfrak{V}_n \cap \mathcal{O}$.

As we have seen, the cusp forms on $\mathfrak{S}_r^p$ of weight k with respect to $\Gamma_{r\lambda}$ can be characterized, if $k > 2n$, as precisely constituting $\mathfrak{H}_{\Gamma_{r\lambda}'}{}^1(k)$, and just as in [12, p. 10-20] this space is just the space of Poincaré series of a certain weight. By the existence theorem of [12, p. 10-44] it is known for given m that if $a_1, \cdots, a_l$ are pairwise incongruent points of $\mathfrak{S}_r^p \bmod \Gamma_{r\lambda}'$ and if k is a sufficiently large multiple of an integer k_0 depending only on $\Gamma_{r\lambda}'$, then the Poincaré series of weight k span the direct sum of the residue classes of (invariant) power series modulo the m-th power of the maximal ideal (of invariant power series) at $a_1, \cdots, a_l$. From these facts we have the following

THEOREM 2. *Let $a_1, \cdots, a_l \in \mathfrak{S}_r^p$ be pairwise incongruent* $\bmod\, \Gamma_{r\lambda}'$ *and let m be a positive integer. Then if k is a sufficiently large multiple of k_0, there exists $f \in \mathcal{S}_{\Gamma_{r\lambda}'}(k)$ having preassigned (invariant) power series developments at $a_1, \cdots, a_l$ up to and including terms of degree $m-1$.*

Since $\mathcal{S}_r \subset \Phi_{(r)}{}^n(\mathfrak{H}_n)$, we have the obvious

COROLLARY. *Let $x \in \mathfrak{V}_{r\lambda}$. Then if k is a sufficiently large multiple of k_0, there exist $f_0, \cdots, f_q \in \mathfrak{H}_n$ such that*

(1) $(\Phi_{r\lambda}{}^n f_0)(x) \neq 0$.

(2) *x is an isolated point of the variety of common zeros of*

$$\Phi_{r\lambda}{}^n f_1, \cdots, \Phi_{r\lambda}{}^n f_q.$$

(3) $\Phi_{(r+1)}{}^n f_j = 0$, $j = 0, \cdots, q$, *and* $\Phi_{r\lambda'}{}^n f_j = 0$, $j = 0, \cdots, q$ if $\lambda' \neq \lambda$.

Let $x \in \mathfrak{V}_{r\lambda}$, let $f_0, \cdots, f_s$ be chosen as in the above Corollary, and let $\mathcal{U}$ be a compact neighborhood of x on $\mathfrak{V}_n^*$ such that $f_0 \neq 0$ on $\mathcal{U}$. If $r \leqq r' \leqq n$, let $\mathcal{U}_{r'} = \bigcup_{\lambda'} \mathfrak{V}_{r'\lambda'} \cap \mathcal{U}$.

If $f_1, \cdots, f_k$ are functions on an open set $\mathcal{O}$, we let

$$V(f_1, \cdots, f_k) = \{z \,|\, z \in \mathcal{O}, f_1(z) = \cdots = f_k(z) = 0\}.$$

THEOREM 3. *The $\mathfrak{A}$-functions on $\mathcal{U}$ separate the points of $\mathcal{U}$. For each*

s, ν, $n \geqq s \geqq r$, there exists a finite number of $\mathfrak{A}$-functions $g_1, \cdots, g_t$ on $\mathcal{U}$ such that $V(g_1, \cdots, g_t) = \operatorname{clos}(\mathfrak{B}_{s\nu} \cap \mathcal{U})$.

Proof. We prove the last part of the theorem first by induction on $n - s$. This part is trivial if $s = n$. Suppose it has been proved for $s + 1$. Let ν' be such that $\operatorname{clos}(\mathfrak{B}_{s\nu}) \cap \mathcal{U} \subset \operatorname{clos}(\mathfrak{B}_{s+1\, \nu'}) \cap \mathcal{U}$, and let $g_1, \cdots, g_{t_1}$ be $\mathfrak{A}$-functions on $\mathcal{U}$ such that $V(g_1, \cdots, g_{t_1}) = \operatorname{clos}(\mathfrak{B}_{s+1\, \nu'}) \cap \mathcal{U}$. If $y \in \operatorname{clos}(\mathfrak{B}_{s+1\, \nu'}) \cap \mathcal{U} - \operatorname{clos}(\mathfrak{B}_{s\nu})$, there exists an $\mathfrak{A}$-function g on $\mathcal{U}$ such that $\mathfrak{B}_{s\nu} \subset V(g)$, $g(y) \neq 0$. In fact, either $y \in \mathfrak{B}_{s+1, \nu'}$, in which case there exists $h \in \mathcal{S}_{s+1\, \nu'}(l)$, for some sufficiently large multiple l of k_0, such that $h(y) \neq 0$ and there exists $f \in \mathfrak{H}_n$ such that $\Phi_{s+1\, \nu'}{}^n f = h$, or else $y \in \mathfrak{B}_{s, \nu''}$, $\nu'' \neq \nu$, and there exists $f \in \mathfrak{H}_n$ such that $\Phi_{s\nu}{}^n \equiv 0$, $(\Phi_{s\nu''}{}^n f)(y) \neq 0$; in either case some power of f divided by a suitable power of f_0 is the desired $\mathfrak{A}$-function g. If $g_1, \cdots, g_{t_1}, g_{t_1+1}, \cdots, g_t$ are $\mathfrak{A}$-functions on $\mathcal{U}$ such that $\mathfrak{B}_{s\nu} \subset V(g_1, \cdots, g_t)$, $V(g_1, \cdots, g_t) - \mathfrak{B}_{s\nu}$ consists of a certain countable number of irreducible analytic spaces. Let $g_{t_1+1}, \cdots, g_t$ be chosen such that the highest dimension of any of these is as small as possible. We assert that then $V(g_1, \cdots, g_t) = \mathfrak{B}_{s\nu}$. In fact, suppose this were not the case and let $V_1, V_2, \cdots$, be all the components of $V(g_1, \cdots, g_t) - \mathfrak{B}_{s\nu}$ of highest dimension $= d$, and let $p_i \in V_i$, $i = 1, 2, \cdots$. We know there exists an $\mathfrak{A}$-function $g^{(i)}$ in $\mathcal{U}$ such that $g^{(i)}(p_i) \neq 0$, $\mathfrak{B}_{s\nu} \subset V(g^{(i)})$. Then (just as in [12]) we can construct a uniformly convergent series $\sum c_i g^{(i)} = g$, c_i constants, such that $g(p_i) \neq 0$, $i = 1, 2, \cdots$. Since the dimension of the highest dimensional component of $V(g_1, \cdots, g_t) - \mathfrak{B}_{s\nu}$ must now be strictly less than d, we have arrived at a contradiction. This completes the proof of the last part of the theorem.

Now let $y_1, y_2 \in \mathcal{U}$. Suppose $y_1 \in \mathfrak{B}_{r_1\lambda_1}$, $y_2 \in \mathfrak{B}_{r_2\lambda_2}$. It is an immediate consequence of the corollary to the preceding theorem that if $r_1 > r_2$ or if $r_1 = r_2$, $\lambda_1 \neq \lambda_2$, then for suitable l there exists $f \in \mathfrak{H}_n(l)$ such that $\Phi_{r_1\lambda_1}{}^n f(y_1) \neq 0$, $\Phi_{r_2\lambda_2}{}^n f(y_2) = 0$. If $y_1, y_2 \in \mathfrak{B}_{r_1\lambda_1}$, then there exists $h \in S_{r_1\lambda_1}(l)$ such that $h(y_1) \neq 0$, $h(y_2) = 0$, and there exists $f \in \mathfrak{H}_n$ such that $\Phi_{r_1\lambda_1}{}^n f = h$. In either case, a suitable power of f divided by some power of f_0 is an $\mathfrak{A}$-function g on $\mathcal{U}$ such that $g(y_1) \neq g(y_2)$.

COROLLARY. *There exists a finite set of $\mathfrak{A}$-functions $g_1, \cdots, g_N$ on $\mathcal{U}$ such that for suitable integers $1 < l_{n-1} < l_{n-2} < \cdots < l_r < l_0 < N$ we have* $V(g_1, \cdots, g_{l_s}) = \mathcal{U}_s$, $n - 1 \leqq s \leqq r$, $V(g_1, \cdots, g_{l_0}) = x$.

Now consider the mapping

$$g : \mathcal{U} \to C^N$$

defined by $g(y) = (g_1(y), \cdots, g_N(y))$. Since $g^{-1}g(x) = x$, this is evidently

a proper mapping if $\mathfrak{U}$ is chosen small enough, and by the preceding Corollary we may assume the images $g(\mathfrak{B}_{s\nu})$, $n \geqq s \geqq r$, are disjoint. Proceeding just as in [1] we may assume, by suitably choosing open neighborhoods $\mathfrak{U}_1$ and $\mathfrak{U}_2$ of x such that $\bar{\mathfrak{U}}_2 \subset \mathfrak{U}_1$, $\bar{\mathfrak{U}}_1 \subset \mathfrak{U}$ we may assume that $g^{-1}(g(\bar{\mathfrak{U}}_2)) \cap \bar{\mathfrak{U}}_1 \subset \mathfrak{U}_1$ and that if $a \in g(\mathfrak{B}_{s\nu} \cap \bar{\mathfrak{U}}_2)$, then $g^{-1}(a) \cap \mathfrak{U}$ is a compact analytic subvariety of $\mathfrak{U}_1 \cap \mathfrak{B}_{s\nu}$, and since the $\mathfrak{A}$-function on $\mathfrak{U}$ separate points, $g^{-1}(a)$ is a finite set of points [1]. Therefore, $g(\mathfrak{B}_{s\nu} \cap \mathfrak{U}_2)$ is an analytic variety of dimension $\frac{1}{2}ps(s+1)$ in a neighborhood of each of its points. It therefore follows from a theorem of Remmert and Stein [15] by an obvious procedure of induction that $g(\mathfrak{U}_2)$ is an analytic variety of dimension $\frac{1}{2}pn(n+1)$ in a neighborhood $\mathfrak{N}$ of $g(x)$, and the inverse image of each of an everywhere dense set of points of $g(\mathfrak{U}_2) \cap \mathfrak{N}$ consists of exactly d points for some positive integer d. Then, just as in [1], we can make $d=1$ by an appropriate choice of $g_1, \cdots, g_N$, because the $\mathfrak{A}$-functions on $\mathfrak{U}$ separate points. On the other hand, each point y of $\mathfrak{U}$ has a basis of neighborhoods $\{\mathfrak{U}_\alpha\}$ such that $\mathfrak{U}_\alpha \cap \mathfrak{U}_n$ is an irreducible analytic variety, and by our definition of $\mathfrak{A}$-function it follows easily [12 exposé 15] that the ring $\mathfrak{A}_y$ of germs of $\mathfrak{A}$-functions at y is integrally closed. Moreover, it follows for the same reasons as in the place cited that $g(\mathfrak{U}_2)$ is irreducible at $g(x)$. If $y_1, y_2 \in \mathfrak{U}_2$ are such that $g(y_1) = g(y_2)$, and if $\mathfrak{V}_1$ and $\mathfrak{V}_2$ are small connected neighborhoods of y_1 and y_2 respectively, it is clear that $g(\mathfrak{V}_1)$ and $g(\mathfrak{V}_2)$ define distinct irreducible germs of varieties at $g(y_1) = g(y_2)$. Therefore, there is a natural homeomorphism of $\mathfrak{U}_2 \cap g^{-1}(\mathfrak{N})$ with the canonical normal model of $g(\mathfrak{U}_2) \cap \mathfrak{N}$ which preserves the ringed structure [1]. Hence, provided with the given ringed structure of $\mathfrak{A}$-functions, $\mathfrak{U}_2$ is a normal general analytic space. It follows at once that $\mathfrak{B}_n{}^*$ is a normal, general analytic space.

Let k be a multiple of k_0 and let $\phi_0, \cdots, \phi_{N(k)}$ be a basis of the modular forms of weight k. We let $V(k)$ denote the variety of common zeros of $\phi_0, \cdots, \phi_{N(k)}$. Then we can find an increasing sequence of integers $k_0 \mid k_1 \mid \cdots \mid k_n \mid k_{n+1} \mid \cdots$ such that $V(k_i) \supset V(k_{i+1})$, $i = 0, 1, \cdots$. Since $\mathfrak{B}_n{}^*$ is a compact general analytic space, there exists n_0 such that $V(k_{n_0}) = V(k_{n_0+1}) = \cdots$. From the Corollary of Theorem 2 it follows that if $x \in \mathfrak{B}_n{}^*$ and if k is a sufficiently large multiple of k_0, then there exists a modular form ϕ of weight k such that $\phi(x) \neq 0$. Therefore $V(k_{n_0})$ is empty. We denote k_{n_0} again by k_0 and in what follows assume that k is always a multiple of k_0. Since $V(\phi_0, \cdots, \phi_{N(k)})$ is empty, we may define a mapping $\Psi_k\colon \mathfrak{B}_n{}^* \to CP^{N(k)}$, where $CP^{N(k)}$ is the complex projective space of dimension $N(k)$, by $\Psi_k(x) = (\phi_0(x), \cdots, \phi_{N(k)}(x))$. Let

$$\theta_k\colon \mathfrak{B}_n{}^* \times \mathfrak{B}_n{}^* \to CP^{N(k)} \times CP^{N(k)}$$

be defined by $\theta_k = \Psi_k \times \Psi_k$. Let Δ_k be the diagonal of $CP^{N(k)} \times CP^{N(k)}$ and let $D_k = \theta_k^{-1}(\Delta_k)$. D_k is a subvariety of $\mathfrak{B}_n^* \times \mathfrak{B}_n^*$. If $k_1, k_2, \cdots$ is a strictly increasing sequence of positive integers such that $k_0 \mid k_1 \mid k_2 \cdots$, it is clear that $D_{k_1} \supseteq D_{k_2} \supseteq \cdots$, so that for sufficiently large N we have $D_{k_N} = D_{k_{N+1}} = D_{k_{N+2}} = \cdots$. If $x, y \in \mathfrak{B}_{n,p}^*$, there is a modular form ϕ of sufficiently high weight k such that $\phi(x) = 0$, $\phi(y) \neq 0$. This makes it clear that if $\mathfrak{D}$ is the diagonal of $\mathfrak{B}_{n,p}^* \times \mathfrak{B}_{n,p}^*$, we must have $D_{k_n} = \mathfrak{D}$, which means that Ψ_{k_N} is one-to-one.

The holomorphic functions on $\mathfrak{S}_n^p$ form an integrally closed domain of integrity. Therefore [12, p. 17-10] it follows that the integral closure A' of the graded ring A generated by $\phi_0, \cdots, \phi_{N(k)}$ (the elements of degree d are the homogeneous polynomials of degree d in $\phi_0, \cdots, \phi_{N(k)}$) is contained in the set of modular forms of weights which are multiples of k, and is finitely generated (as an algebra over C) since A' is of finite type over A. We know [12, p. 17-05, prop. 4] that there exists an integer d' such that if $A'(d')$ is the graded ring in which the elments of degree h are the automorphic forms in A' of weight hd', then $A'(d')$ is integrally closed and is generated by its elements of degree 1. Letting $g_0, \cdots, g_M$ be a basis of these elements of degree 1, the mapping

$$g: x \to (g_0(x), \cdots, g_n(x))$$

defines a 1-1 holomorphic mapping of $\mathfrak{B}_n^*$ into CP^M. Since $g^{-1}g(a) = a$, the image $g(\mathfrak{B}_n^*)$ is an analytic and therefore (by Chow's theorem) an algebraic variety. Since $A'(d')$ is (naturally identifiable with) the quotient of the algebra of homogeneous polynomials in CP^M by the homogeneous ideal of homogeneous polynomials vanishing on $g(\mathfrak{B}_n^*)$, it follows that $g(\mathfrak{B}_n^*)$ is algebraically and therefore analytically normal. Therefore g, being a one-to-one analytic mapping, is actually an isomorphism of $\mathfrak{B}_n^*$ onto $g(\mathfrak{B}_n^*)$. This completes the proof of

THEOREM 4. *$\mathfrak{B}_n^*$ is complex analytically isomorphic to a normal complex projective variety.*

Since $\dim(\mathfrak{B}_n^* - \mathfrak{B}_n) < \dim(\mathfrak{B}_n^*) - 1$ if $p > 1$, we have, just as in [1, p. 363],

THEOREM 5. *Every meromorphic function on $\mathfrak{S}_n^p$ invariant under Γ' is a quotient of modular forms. (Provided $n > 1$ or $p > 1$.)*

The referee has kindly pointed out to us a recent note [16] in which Pyateckii-Shapiro announces, without proofs, results containing most of the important results of this paper as special cases.

THE UNIVERSITY OF CHICAGO.

REFERENCES.

[1] W. L. Baily, "On Satake's compactification of V_n," *American Journal of Mathematics*, vol. 80 (1958), pp. 348-364.

[2] O. Blumenthal, "Über Modulfunktionen von mehreren Veränderlichen (Erste Hälfte)," *Mathematische Annalen*, vol. 56 (1903), pp. 509-548.

[3] ———, "Über Modulfunktionen von mehreren Veränderlichen (Zweite Hälfte)," *Mathematische Annalen*, vol. 58 (1904), pp. 497-527.

[4] H. Braun, "Konvergenz verallgemeinerter Eisensteiner Reihen," *Mathematische Zeitschrift*, vol. 44 (1939), pp. 387-397.

[5] H. Cartan, "Prolongement des espaces analytiques normaux," *Mathematische Annalen*, vol. 136 (1958), pp. 97-110.

[6] K. F. Gundlach, "Über die Darstellungen der ganzen Spitzenformen, etc.," *Acta Mathematica*, vol. 92 (1954), pp. 309-345.

[7] E. Hecke, "Analytische Funktionen und Algebraische Zahlen, II. Teil," *Abbandlungen aus dem Mathematischen Seminar der Hamburgischen Universität*, vol. 3 (1924), pp. 213-236.

[8] P. Humbert, "Théorie de la réduction des formes quadratiques définies positives dans un corps algébrique K fini," *Commentarii Mathematici Helvetici*, vol. 12 (1939-40), pp. 233-306.

[9] H. Maass, "Zur Theorie der automorphen Funktionen von n Veränderlichen," *Mathematische Annalen*, vol. 117 (1939-1941), pp. 538-578.

[10] I. I. Pyateckii-Shapiro, "Singular Modular Functions," *Izvestia Akademii Nauk* USSR, *Seriya Mathematicheskaya*, vol. 20 (1956), pp. 53-98 (Russian). *AMS Translations*, vol. 10 (1958), pp. 13-58. [The references to page numbers in this paper refer to the AMS translation.]

[11] I. Satake, "On the compactification of the Siegel space," *Journal of the Indian Mathematical Society*, vol. 20 (1956), pp. 259-281.

[12] *Séminaire H. Cartan*, 1957-1958, Mimeographed notes.

[13] C. L. Siegel, *Lectures on the Analytical Theory of Quadratic Forms*, notes by Morgan Ward, Revised Edition, Institute for Advanced Study, 1949.

[14] ———, "Einführung in die Theorie der Modulfunktionen n-ten Grades," *Mathematische Annalen*, vol. 116 (1938-1939), pp. 617-657.

[15] R. Remmert and K. Stein, "Über die wesentliche Singularitäten analytischer Mengen," *Mathematische Annalen*, vol. 126 (1953), pp. 263-306.

[16] I. I. Pyatechkii-Shapiro, "Discrete subgroups of the group of analytic automorphisms of a polycylinder and automorphic forms," *Doklady Akademii Nauk* USSR, vol. 124 (1959), pp. 760-763.

THE LEBESGUE CONTANTS FOR JACOBI SERIES, II.*

By Lee Lorch.[1]

---

1. Introduction and statement of results. This is a direct continuation of Part I [5] whose Introduction outlines the background of this Part as well. The main results presented here are for a narrower range of the parameter α, but, for this range, are substantially more precise. The methods here are different and do not use the result established in Part I.

As before, the Lebesgue constants for Jacobi series (*i. e.*, developments in terms of Jacobi polynomials $P_n^{(\alpha,\beta)}(x)$ at the end-point $x=1$), are written, following H. Rau [6, p. 249, (40)], as

$$L_n(\alpha,\beta)=(\Gamma(n+\alpha+\beta+2)/[\Gamma(\alpha+1)\Gamma(n+\beta+1)]) \cdot \int_0^\pi (\sin\tfrac{1}{2}\theta)^{2\alpha+1}(\cos\tfrac{1}{2}\theta)^{2\beta+1}\,|P_n^{(\alpha+1,\beta)}(\cos\theta)|\,d\theta. \tag{1}$$

An asymptotic expression for $L_n(\alpha,\beta)$ is established in Part I [5, (6)] for $\alpha>-\frac{1}{2}$ and $\beta>-1$, a restriction on β which is imposed throughout this Part as well.

For $\alpha=-\frac{1}{2}$ and $-1<\alpha<-\frac{1}{2}$ the respective results, due to G. Szegö [9, § 20], are recorded without proof in [6] and repeated in [5, (4) and (5)].

Here, [5, (6)] is sharpened for the restricted range $-\frac{1}{2}<\alpha<\frac{1}{2}$, $\alpha-\beta<1$, by replacing the O-terms found there by an explicitly determined constant plus O-terms which are $o(1)$, the detailed statement given by (2). The same is done for [5, (4)], dealing with $\alpha=-\frac{1}{2}$, in (7).

For the first case mentioned, we have

$$L_n(\alpha,\beta)=A_{\alpha\beta}n^{\alpha+\frac{1}{2}}+B_\alpha+O(n^{\alpha-\frac{1}{2}})+O(n^{\alpha-\beta-1}), \tag{2}$$

for $-\frac{1}{2}<\alpha<\frac{1}{2}$ *and* $\alpha-\beta<1$. *Here*

$$A_{\alpha\beta}=2\Gamma(\tfrac{1}{2}\alpha+\tfrac{1}{4})\Gamma(\tfrac{1}{2}\beta+\tfrac{3}{4})/\{\pi^{\frac{3}{2}}\Gamma(\alpha+1)\Gamma(\tfrac{1}{2}[\alpha+\beta]+1)\}, \tag{3}$$

---

* Received December 17, 1958.

[1] This work was supported by the National Science Foundation through Research Grant NSF G-3663 to Philander Smith College. Professor G. Szegö rendered much helpful advice for which I am grateful. I want to thank also the Stanford University Mathematics Department for the facilities it provided while this research was being conducted.

and

$$B_\alpha = \{2^{-\alpha}/\Gamma(\alpha+1)\}\{M_1(\alpha) + \int_0^{j_1} x^\alpha J_{\alpha+1}(x)\,dx$$

$$(4) \qquad + 2\alpha \sum_{k=1}^{\infty} (-1)^k \int_{j_k}^{j_{k+1}} x^{\alpha-1} J_\alpha(x)\,dx$$

$$+ 2\sum_{k=1}^{\infty} [M_{k+1}(\alpha) - (2^{\frac{1}{2}}/\pi^{\frac{1}{2}}) \int_{j_{k-1}}^{j_k} x^{\alpha-\frac{1}{2}}\,dx]\},$$

where both infinite series are absolutely convergent.

In (4), $J_\nu(x)$ is the Bessel function of first kind and ν-th order, $j_n \equiv j_{\alpha+1,n}$ the n-th positive zero[2] of $J_{\alpha+1}(x)$, $n = 1, 2, \cdots, j_0 = 0$, and

$$(5) \qquad M_k(\alpha) \equiv (-1)^k j_{\alpha+1,k}{}^\alpha J_\alpha(j_{\alpha+1,k}) > 0, \qquad k = 1, 2, \cdots.$$

$M_k(\alpha)$ is positive, as stated, since the zeros of $J_\alpha(x)$ and $J_{\alpha+1}(x)$ are interlaced [11, p. 479], *i.e.*, $j_{\alpha 1} < j_{\alpha+1,1} < j_{\alpha 2} < \cdots$, and $(-1)^k J_\alpha(j_{\alpha+1,k}) > 0$.

It is noteworthy that the constant term (4) in (2) is independent of β.

In the important particular case of Laplace series (*i. e.*, developments in terms of Legendre polynomials at the endpoint $x = 1$), $\alpha = \beta = 0$, and (2) becomes

$$L_n(0,0)$$

$$(6)^3 \qquad = 2(2/\pi)^{\frac{1}{2}} n^{\frac{1}{2}} + 1 + 2\sum_{k=1}^{\infty} \{M_k(0) - (2^{\frac{3}{2}}/\pi)(k^{\frac{1}{2}} - [k-1]^{\frac{1}{2}})\}$$

$$+ O(n^{-\frac{1}{2}}).$$

Here $M_k(0)$ can be interpreted as the ordinate of the k-th positive extremum (turning-point) of $|J_0(x)|$, inasmuch as the extrema of $J_0(x)$ occur at the zeros of $J_1(x)$ since $J_0'(x) = -J_1(x)$.

The constant term in (6) has a somewhat different appearance from that

[2] The customary designation, $j_{\alpha+1,n}$, is avoided in the limits of integration for typographical reasons.

[3] The principal term in (6) is due to T. H. Gronwall [1, 2], whose remainder term was $o(n^{\frac{1}{2}})$. His proofs were rather complicated; simpler ones were devised by G. Szegö [7, 8].

The constant term in (6) was suggested to me by Szegö, along with the outline of a proof. (The value I announced in abstract 544-18, *Notices of the American Mathematical Society*, vol. 5, 1958, p. 212, is incorrect.) A proof of (6) can be given without the full argumentation needed for (2); (15) and (18) can be joined together directly through the familiar asymptotic formula applied to $J_0(x)$ and $J_1(x)$ without the intervention of the Lemma of § 2.

which is obtained on putting $\alpha = 0$ in (4). The transition is made by rewriting the second infinite series in (4) in this case as

$$\lim_{n\to\infty}\{M_1(0) + \cdots + M_n(0) - (2^{\frac{1}{2}}/\pi^{\frac{3}{2}}) \int_0^{j_{1n}} x^{-\frac{1}{2}}\, dx\}$$
$$= \lim_{n\to\infty}\{M_1(0) + \cdots + M_n(0) - (2^{\frac{3}{2}}/\pi) n^{\frac{1}{2}}\},$$

in view of (31) below, since, for $\alpha = 0$,

$$\int_0^{j_1} x^\alpha J_{\alpha+1}(x)\, dx = \int_0^{j_{11}} J_1(x)\, dx = J_0(0) - J_0(j_{11})$$
$$= 1 + M_1(0).$$

The more precise version of [5, (4)] is:

$$L_n(-\tfrac{1}{2}, \beta) = (4/\pi^2)\log n + C_\beta + O(n^{-1}\log n) + O(n^{-\beta-\frac{3}{2}}), \tag{7}$$

where

$$C_\beta = (4/\pi^2)\log 2 + (2/\pi) \int_0^1 \theta^{-1}\sin\theta\, d\theta$$
$$- (4/\pi^2) \int_0^{\frac{1}{2}\pi} (\{1 - (\cos\theta)^{\beta+\frac{1}{2}}\}/\sin\theta)\, d\theta \tag{8}$$
$$- (2/\pi) \int_1^\infty \theta^{-1}\{(2/\pi) - |\sin\theta|\}\, d\theta.$$

Putting $\beta = -\frac{1}{2}$ in (7) gives rise to the case of Tchebycheff polynomials (equivalent to ordinary Fourier series; cf. footnote 6 in [5]). In this case (7) and (8) assume the form found for the Lebesgue constants for Fourier series in [3], except for the remainder term.

The discussion of the cases considered here ($\alpha = -\frac{1}{2}$; $-\frac{1}{2} < \alpha < \frac{1}{2}$) is based on (20), a representation of $L_n(\alpha, \beta)$ in terms of Bessel functions. This formula requires for its justification a Lemma permitting the substitution of one (real) solution of Bessel's differential equation for another in certain integrals. This provides the content of § 2. The basic representation (20) is then established in § 3.

Thereafter the cases are handled separately: $\alpha = -\frac{1}{2}$ in § 4 and $-\frac{1}{2} < \alpha < \frac{1}{2}$, $\alpha - \beta < 1$ in § 5. The case $-1 < \alpha < -\frac{1}{2}$ [9, § 20], in which $L_n(x, \beta)$ is bounded, can be handled by the simpler formula (15). This is left to the reader.

2. A lemma on Bessel functions. In deriving (20), the following result is needed. Its final sentence justifies replacing one Bessel function by

another in the integrals involved, without altering either the value of the limit or the magnitudes of the remainder terms.

LEMMA.[4] *For* $0 < \epsilon < \pi$, $\nu > -1$, *define*

$$(9)\qquad S_N(\alpha,\beta) = N^{\alpha+1}\int_{\pi-\epsilon}^{\pi-1/N}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}}\,|\,\mathscr{C}_\nu(N\theta,\delta)\,|\,d\theta$$

and

$$(10)\qquad S_N'(\alpha,\beta) = N^{\alpha+1}\int_{\pi-\epsilon}^{\pi}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}}\,|\,\mathscr{C}_\nu(N\theta,\delta)\,|\,d\theta,$$

where[5] $\mathscr{C}_\nu(x,\delta) = J_\nu(x)\cos\pi\delta - Y_\nu(x)\sin\pi\delta$.

Then

$$(11)\qquad \begin{aligned} S_N(\alpha,\beta) = (2/\pi^{\frac{3}{2}})N^{\alpha+\frac{1}{2}}&\int_{\pi-\epsilon}^{\pi-1/N}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}\,d\theta \\ &+ O(N^{\alpha-\frac{1}{2}}) + O(N^{\alpha-\beta-1}), \end{aligned}$$

and

$$(12)\qquad \begin{aligned} S_N'(\alpha,\beta) = (2/\pi^{\frac{3}{2}})N^{\alpha+\frac{1}{2}}&\int_{\pi-\epsilon}^{\pi}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}\,d\theta \\ &+ O(N^{\alpha-\frac{1}{2}}) + O(N^{\alpha-\beta-1}). \end{aligned}$$

In both (11) *and* (12), *the expressions on the right are independent of (fixed)* ν *and* δ.

Proof of (11). Hankel's asymptotic formula [11, p. 488] for $\mathscr{C}_\nu(N\theta,\delta)$ shows that, for $\theta \geqq \pi-\epsilon$, $(\tfrac{1}{2}\theta)^{\frac{1}{2}}\mathscr{C}_\nu(N\theta,\delta) = (\pi N)^{-\frac{1}{2}}\cos(N\theta+\gamma) + O(N^{-\frac{3}{2}})$, where $\gamma = \delta - \tfrac{1}{2}\nu\pi - \pi/4$. Using it in (9), we see that its remainder term contributes to $S_N(\alpha,\beta)$ an amount which is $O(N^{\alpha-\frac{1}{2}})$.

Thus, (11) will be established once it is shown that $|\cos(N\theta+\gamma)|$ can be replaced by its mean value $2/\pi$ with an additive error $O(N^{\alpha-\frac{1}{2}}) + O(N^{\alpha-\beta-1})$. This, in turn, is an immediate consequence of Theorem 2.1 of [4, p. 90], whose hypotheses can be verified readily for the case at hand. (Cf. [5, § 3, Remark].)

Proof of (12). As in the proof of (11), it is clear that the remainder term in Hankel's asymptotic formula contributes only $O(N^{\alpha-\frac{1}{2}})$ to $S_N'(\alpha,\beta)$. To complete the proof of (12), therefore, it is plainly sufficient to show that

---

[4] This Lemma is valid without any restriction on α, provided $\beta > -\frac{3}{2}$, *i. e.*, under broader conditions than the requirements $\alpha > -1$, $\beta > -1$ placed throughout both Parts.

[5] This is a minor adaptation of the usual notation for real cylinder functions; $Y_\nu(x)$ is the Bessel function of second kind and ν-th order.

the contribution of the integral over $(\pi - 1/N, \pi)$ involving the principal term does not exceed the error terms stated in (12); this is a straightforward calculation, which is left to the reader.

3. Representation of $L_n(\alpha, \beta)$ in terms of Bessel functions. In this section, the integrand in (1) is replaced by an asymptotic representation (20) in terms of Bessel functions, on which the proofs of (2) and (7) are based. This change can be accomplished by means of an asymptotic formula, due to G. Szegö, of "Hilb type" [10, p. 191, Theorem 8.21.12]. However, this requires decomposing the integral (1) into the sum of two integrals $(0 < \epsilon < \pi)$

$$L_n(\alpha, \beta) = \int_0^{\pi-\epsilon} + \int_{\pi-\epsilon}^{\pi} \equiv L_{n1}(\alpha, \beta) + L_{n2}(\alpha, \beta), \tag{13}$$

where the factor preceding the integral sign in (1) is understood to precede each of the integral signs in (13).

Szegö's formula can be applied directly to the integrand of $L_{n1}(\alpha, \beta)$. Doing so yields

$$\begin{aligned}(\sin \tfrac{1}{2}\theta)^{2\alpha+1}(\cos \tfrac{1}{2}\theta)^{2\beta+1}&P_n^{(\alpha+1,\beta)}(\cos\theta) \\ &= (\Gamma(n+\alpha+2)/N^{\alpha+1}n!)(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}}J_{\alpha+1}(N\theta) \\ &\quad + \begin{cases}\theta^{\alpha+\frac{1}{2}}O(n^{-\frac{3}{2}}), & 1/n \leqq \theta \leqq \pi - \epsilon, \\ \theta^{2\alpha+3}O(n^{\alpha+1}), & 0 < \theta \leqq 1/n,\end{cases}\end{aligned} \tag{14}$$

where $N = n + \frac{1}{2}(\alpha + \beta + 2)$, a notation which is retained throughout.

The remainder term in (14) contributes $O(n^{\alpha-\frac{1}{2}})$ to $L_n(\alpha, \beta)$, from (1), as may be seen from Stirling's formula.

Next, when the factor not involving θ in the principal term of (14) is combined with the factor preceding the integral sign in (13) [the same as in (1)], the resulting product is

$$\{\Gamma(n+\alpha+\beta+2)\Gamma(n+\alpha+2)\}/\{N^{\alpha+1}n!\Gamma(\alpha+1)\Gamma(n+\beta+1)\}.$$

This is, from Stirling's formula, $N^{\alpha+1}/\Gamma(\alpha+1) + O(n^\alpha)$, since $N - n$ is a constant.

Thus,

$$\begin{aligned}L_{n1}(\alpha, \beta) &= \{N^{\alpha+1}/\Gamma(\alpha+1) + O(n^\alpha)\} \\ &\quad \cdot \int_c^{\pi-\epsilon} (\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}} \,|\, J_{\alpha+1}(N\theta) \,|\, d\theta + O(n^{\alpha-\frac{1}{2}}).\end{aligned} \tag{15}$$

In $L_{n2}(\alpha,\beta)$ it is helpful to replace θ by $\pi-\phi$, so that in view of [10, p. 58, (4.1.3)],

$$(16)\qquad \begin{aligned} L_{n2}(\alpha,\beta) &= (\Gamma(n+\alpha+\beta+2)/\Gamma(\alpha+1)\Gamma(n+\beta+1)) \\ &\cdot \int_0^{\epsilon} (\sin\tfrac{1}{2}\phi)^{2\beta+1}(\cos\tfrac{1}{2}\phi)^{2\alpha+1} \mid P_n^{(\beta,\alpha+1)}(\cos\phi)\mid d\phi. \end{aligned}$$

In this case Szegö's formula [10, p. 191, Theorem 8.12.12] becomes

$$(17)\qquad \begin{aligned} &(\sin\tfrac{1}{2}\phi)^{2\beta+1}(\cos\tfrac{1}{2}\phi)^{2\alpha+1}P_n^{(\beta,\alpha+1)}(\cos\phi) \\ &= (N^{-\beta}\Gamma(n+\beta+1)/n!)(\sin\tfrac{1}{2}\phi)^{\beta+\frac{1}{2}}(\cos\tfrac{1}{2}\phi)^{\alpha-\frac{1}{2}}(\tfrac{1}{2}\phi)^{\frac{1}{2}}J_\beta(N\phi) \\ &\quad + \begin{cases} \phi^{\beta+\frac{3}{2}}O(n^{-\frac{3}{2}}), & 1/n \leqq \phi \leqq \pi-\epsilon, \\ \phi^{2\beta+3}O(n^{\beta}), & 0<\phi\leqq 1/n. \end{cases} \end{aligned}$$

As in the case of $L_{n1}(\alpha,\beta)$, there is no difficulty in showing that the error terms in (17) contribute $O(n^{\alpha-\beta-3})+O(n^{\alpha-\frac{1}{2}})=O(n^{\alpha-\frac{1}{2}})$ to $L_{n2}(\alpha,\beta)$.

Furthermore, combining the ϕ-free factor in the principal term of (17) with the factor preceding the integral sign in $L_{n2}(\alpha,\beta)$ gives rise to a factor which is $N^{\alpha+1}/\Gamma(\alpha+1)+O(n^{\alpha})$, in the same manner as before.

Reverting now to θ, (17) shows thus that

$$(18)\qquad \begin{aligned} L_{n2}(\alpha,\beta) &= \{N^{\alpha+1}/\Gamma(\alpha+1)+O(n^{\alpha})\} \\ &\cdot \int_{\pi-\epsilon}^{\pi} (\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\{\pi-\theta\})^{\frac{1}{2}} \mid J_\beta(N\{\pi-\theta\})\mid d\theta + O(n^{\alpha-\frac{1}{2}}). \end{aligned}$$

We wish now to replace $(\tfrac{1}{2}\{\pi-\theta\})^{\frac{1}{2}} \mid J_\beta(N\{\pi-\theta\})\mid$ by $(\tfrac{1}{2}\theta)^{\frac{1}{2}}\mid J_{\alpha+1}(N\theta)\mid$ in (18). This can be justified by means of (*a*) Hankel's asymptotic formula [11, p. 488] and (*b*) the Lemma of § 2.

It is convenient to consider separately the cases $\beta=-\frac{1}{2}$ and $\beta\neq-\frac{1}{2}$. For $\beta=-\frac{1}{2}$, [11, pp. 55, 64],

$$\begin{aligned} (\pi-\theta)^{\frac{1}{2}} \mid J_{-\frac{1}{2}}(N\{\pi-\theta\})\mid &= (2/\pi)^{\frac{1}{2}}N^{-\frac{1}{2}}\mid \cos N\theta\mid \\ &= \theta^{\frac{1}{2}}\mid J_{-\frac{1}{2}}(N\theta)\mid = \theta^{\frac{1}{2}}\mid Y_{\frac{1}{2}}(N\theta)\mid = \theta^{\frac{1}{2}}\mid \mathscr{C}_{\frac{1}{2}}(N\theta,-\tfrac{1}{2})\mid \end{aligned}$$

so that

$$(19)\qquad (\tfrac{1}{2}\{\pi-\theta\})^{\frac{1}{2}}\mid J_{-\frac{1}{2}}(N\{\pi-\theta\})\mid = (\tfrac{1}{2}\theta)^{\frac{1}{2}}\mid \mathscr{C}_{\frac{1}{2}}(N\theta,-\tfrac{1}{2})\mid.$$

Using (19) and the Lemma of § 2 (whose final sentence permits replacing $\mathscr{C}_{\frac{1}{2}}(N\theta,-\frac{1}{2})$ by $J_{\alpha+1}(N\theta)$), the integrand on the right of (18) becomes identical with that in (15) with an error of $O(n^{\alpha-\beta-1})+O(n^{\alpha-\frac{1}{2}})$.

Hence, for $\beta=-\frac{1}{2}$, we have from (13),

$$(20)\qquad \begin{aligned} L_n(\alpha,\beta) &= \{N^{\alpha+1}/\Gamma(\alpha+1)+O(n^{\alpha})\} \\ &\cdot \int_0^{\pi} (\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}}\mid J_{\alpha+1}(N\theta)\mid d\theta + O(n^{\alpha-\beta-1}) + O(n^{\alpha-\frac{1}{2}}). \end{aligned}$$

The same formula is valid also when $\beta \neq -\frac{1}{2}$. To show this, it is helpful to decompose $L_{n2}(\alpha, \beta)$:

$$L_{n2}(\alpha,\beta) = \{N^{\alpha+1}/\Gamma(\alpha+1) + O(n^{\alpha})\}\left\{\int_{\pi-\epsilon}^{\pi-1/N} + \int_{\pi-1/N}^{\pi}\right\} \tag{21}$$
$$\equiv L_{n2}'(\alpha,\beta) + L_{n2}''(\alpha,\beta).$$

Now,

$$L_{n2}''(\alpha,\beta) = O(n^{\alpha+1})\int_{\pi-1/N}^{\pi}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\pi-\theta)^{\frac{1}{2}}\,|\,J_\beta(N\{\pi-\theta\})\,|\,d\theta$$
$$= O(n^{\alpha+1})\int_0^{1/N}(\sin\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}\theta^{\frac{1}{2}}\,|\,J_\beta(N\theta)\,|\,d\theta$$
$$= O(n^{\alpha+\beta+1})\int_0^{1/N}\theta^{2\beta+1}\,d\theta = O(n^{\alpha-\beta-1}),$$

since $J_\beta(N\theta) \sim N^\beta\theta^\beta$ for $N\theta$ small [10, p. 16, (1.71.10)].

To L_{n2}', Hankel's asymptotic formula [11, p. 488] may be applied. This implies, for $\pi-\epsilon \leqq \theta \leqq \pi - 1/N$,

$$(\tfrac{1}{2}\{\pi-\theta\})^{\frac{1}{2}}\,|\,J_\beta(N\{\pi-\theta\})\,| = (\tfrac{1}{2}\theta)^{\frac{1}{2}}\,|\,\mathscr{B}_{\beta+1}(N\theta,\beta)\,| + (\pi-\theta)^{-1}O(N^{-\frac{3}{2}}), \tag{22}$$

a result which takes the more precise form (19) when $\beta = -\frac{1}{2}$.

For $\beta \neq -\frac{1}{2}$, the remainder term in (22) contributes to $L_{n2}'(\alpha,\beta)$ an amount which is $O(n^{\alpha-\beta-1}) + O(n^{\alpha-\frac{1}{2}})$.

Thus,

$$L_{n2}(\alpha,\beta) = \{N^{\alpha+1}/\Gamma(\alpha+1) + O(n^{\alpha})\}$$
$$\cdot\int_{\pi-\epsilon}^{\pi-1/N}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}}\,|\,\mathscr{B}_{\beta+1}(N\theta,\beta)\,|\,d\theta$$
$$+ O(n^{\alpha-\beta-1}) + O(n^{\alpha-\frac{1}{2}}).$$

The expression corresponding to the right member of this last equation with the limits of integration replaced by $\pi - 1/N$ and π is $O(n^{\alpha-\beta-1}) + O(n^{\alpha-\frac{1}{2}})$, as shown by the same argument used to establish (12). Hence,

$$L_{n2}(\alpha,\beta) = \{N^{\alpha+1}/\Gamma(\alpha+1) + O(n^{\alpha})\}$$
$$\cdot\int_{\pi-\epsilon}^{\pi}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}(\tfrac{1}{2}\theta)^{\frac{1}{2}}\,|\,\mathscr{B}_{\beta+1}(N\theta,\beta)\,|\,d\theta$$
$$+ O(n^{\alpha-\beta-1}) + O(n^{\alpha-\frac{1}{2}}).$$

To this the Lemma of § 2 applies, showing that the replacement of $|\,\mathscr{B}_{\beta+1}(N\theta,\beta)|$ by $|\,J_{\alpha+1}(\theta)|$ in the integrand does not affect the value of $L_{n2}(\alpha,\beta)$ beyond the error stated in (12). This substitution made, (13) shows that (20) *is valid also for* $\beta \neq -\frac{1}{2}$*, as well as for* $\beta = -\frac{1}{2}$.

4. The case $\alpha = -\frac{1}{2}$; proof of (7). When $\alpha = -\frac{1}{2}$, (20) becomes [11, p. 55]

$$L_n(-\tfrac{1}{2},\beta) = \{2/\pi + O(n^{-1})\} \cdot \int_0^{\frac{1}{2}\pi} \{(\cos\theta)^{\beta+\frac{1}{2}} \,|\sin 2N\theta\,|/\sin\theta\}\,d\theta + O(n^{-\beta-\frac{3}{2}}) + O(n^{-1}). \tag{23}$$

The desired asymptotic expression for $L_n(-\frac{1}{2},\beta)$ is obtained by comparing the integral on the right of (23) with the extension to non-integral N of the Lebesgue constants for Fourier series (cf. [4, Theorem 4.1, p. 96]), essentially $L_n(-\frac{1}{2},-\frac{1}{2})$. Obviously, it suffices to consider $\beta \neq -\frac{1}{2}$ below.

In order to include the case in which $\beta + \frac{1}{2}$ is negative, it is convenient to decompose the integral in question into the sum of two integrals, over $(0, \frac{1}{2}\pi - \pi/(2N))$ and $(\frac{1}{2}\pi - \pi/(2N), \frac{1}{2}\pi)$, say $\rho_{n1}(-\frac{1}{2},\beta)$ and $\rho_{n2}(-\frac{1}{2},\beta)$, respectively.

It is easy to show that $\rho_{n2}(-\frac{1}{2},\beta) = O(N^{-\beta-\frac{3}{2}})$, an amount which can be absorbed in the error terms already found in (23).

Hence it is sufficient to consider $\rho_{n1}(-\frac{1}{2},\beta)$.

Now,

$$\begin{aligned}(2/\pi)\int_0^{\frac{1}{2}\pi-\pi/(2N)} &(\{1-(\cos\theta)^{\beta+\frac{1}{2}}\}\,|\sin 2N\theta\,|/\sin\theta)\,d\theta \\ &= (4/\pi^2)\int_0^{\frac{1}{2}\pi-\pi/(2N)} (\{1-(\cos\theta)^{\beta+\frac{1}{2}}\}/\sin\theta)\,d\theta + O(N^{-\beta-\frac{3}{2}}) + O(N^{-1})\end{aligned} \tag{24}$$

from Theorem 2.1 of [4], since the mean value of $|\sin\theta|$ is $2/\pi$.

Thus,

$$\begin{aligned}L_n(-\tfrac{1}{2},\beta) = (2/\pi)&\int_0^{\frac{1}{2}\pi-\pi/(2N)} (|\sin 2N\theta\,|/\sin\theta)\,d\theta \\ &-(4/\pi^2)\int_0^{\frac{1}{2}\pi-\pi/(2N)} (\{1-(\cos\theta)^{\beta+\frac{1}{2}}\}/\sin\theta)\,d\theta + O(N^{-\beta-\frac{3}{2}}) + O(N^{-1}),\end{aligned} \tag{25}$$

and from this it follows easily that

$$\begin{aligned}L(-\tfrac{1}{2},\beta) = \{(2/\pi) + O(n^{-1})\}&\int_0^{\frac{1}{2}\pi} (|\sin 2N\theta\,|/\sin\theta)\,d\theta \\ &-(4/\pi^2)\int_0^{\frac{1}{2}\pi} (\{1-(\cos\theta)^{\beta+\frac{1}{2}}\}/\sin\theta)\,d\theta + O(N^{-\beta-\frac{3}{2}}) + O(N^{-1}).\end{aligned} \tag{26}$$

The first integral on the right in (26) is the extension to non-integral values of the n-th Lebesgue constant in Fourier series. This is directly covered by Theorem 4.1 of [4, p. 96], whose use completes the proof of (7) since $N - n$ is a constant, namely $\frac{1}{2}(\beta + \frac{3}{2})$.

5. The case $-\frac{1}{2} < \alpha < \frac{1}{2}$, $\alpha - \beta < 1$; proof of (2). In this case, the remainder term in the factor of the integral on the right of (20) induces a contribution to $L_n(\alpha,\beta)$ which is $O(n^{\alpha-\frac{1}{2}})$ and hence absorbable in the error terms already present in (20). This can be shown by estimates of the same type as have already been made frequently in previous sections. In carrying them out, it is convenient to write $L_n(\alpha,\beta) = L_{n1}(\alpha,\beta) + L_{n2}(\alpha,\beta)$ again and to use the representation (18) for $L_{n2}(\alpha,\beta)$. Alternatively, this can be held in abeyance, to appear incidentally in the forthcoming estimate of the integral on the right of (20).

In any event, the factor of that integral may as well be taken as $N^{\alpha+1}/\Gamma(\alpha+1)$ from the outset, thus simplifying the notation. This done, (20) can be written as follows:

$$L_n(\alpha,\beta) = \{N^{\alpha+1}/\Gamma(\alpha+1)\} \int_0^{\pi} f_{\alpha\beta}(\theta)\theta^{-\alpha} \,|\, J_{\alpha+1}(N\theta) \,|\, d\theta + O(n^{\alpha-\frac{1}{2}}) + O(n^{\alpha-\beta-1}), \tag{27}$$

where

$$f_{\alpha\beta}(\theta) = (\tfrac{1}{2}\theta \cot \tfrac{1}{2}\theta)^{\frac{1}{2}}(\theta \sin \tfrac{1}{2}\theta)^{\alpha}(\cos \tfrac{1}{2}\theta)^{\beta}. \tag{28}$$

Now [11, p. 45], $D_x\{x^{-\alpha}J_\alpha(x)\} = -x^{-\alpha}J_{\alpha+1}(x)$. Hence, integrating by parts and writing $x = N\theta$, $N\theta_k = j_{\alpha+1,k}$ with $0 \leqq \theta < \pi$, $0 \leqq \theta_k < \pi$, we have

$$\begin{aligned} N \int_{\theta_k}^{\theta_{k+1}} & f_{\alpha\beta}(\theta)\theta^{-\alpha}J_{\alpha+1}(N\theta)\, d\theta \\ &= f_{\alpha\beta}(\theta_k)\theta_k^{-\alpha}J_\alpha(j_{\alpha+1,k}) - f_{\alpha\beta}(\theta_{k+1})\theta_{k+1}^{-\alpha}J_\alpha(j_{\alpha+1,k+1}) \\ &\quad + \int_{\theta_k}^{\theta_{k+1}} f_{\alpha\beta}'(\theta)\theta^{-\alpha}J_\alpha(N\theta)\, d\theta, \end{aligned}$$

where $J_{\alpha+1}(N\theta)$ is of constant sign $(-1)^k$ in the interval of integration.

Furthermore,

$$\begin{aligned} N^{\alpha+1} \int_0^{\theta_1} & f_{\alpha\beta}(\theta)\theta^{-\alpha} \,|\, J_{\alpha+1}(N\theta) \,|\, d\theta \\ &= 2^{-\alpha} \int_0^{j_1} \{(t/[2N])/\tan(t/[2N])\}^{\frac{1}{2}}\{\sin(t/[2N])/(t/[2N])\}^{\alpha} \\ &\qquad \cdot \{\cos(t/[2N])\}^{\beta} t^{\alpha} J_{\alpha+1}(t)\, dt \\ &= 2^{-\alpha} \int_0^{j_1} t^{\alpha} J_{\alpha+1}(t)\, dt + O(n^{-2}), \end{aligned}$$

since $J_{\alpha+1}(t) > 0$ in the interval of integration, and the factor of $t^{\alpha}J_{\alpha-1}(t)$ in the next to last integral is an even analytic function assuming the value 1 at the origin and hence representable as $1 + O(t^2/N^2)$.

Thus, (27) can be written as

$$
\begin{aligned}
L_n(\alpha,\beta) &= (2^{-\alpha}/\Gamma(\alpha+1))\{\int_0^{j_1} t^\alpha J_{\alpha+1}(t)\,dt \\
&\quad + 2\sum_{k=2}^{[N]-1} g_{\alpha\beta}(\theta_k)M_k(\alpha) + g_{\alpha\beta}(\theta_1)M_1(\alpha) \\
&\quad + g_{\alpha\beta}(\theta_{[N]})M_{[N]}(\alpha)\} + (N^\alpha/\Gamma(\alpha+1))\int_{\theta_{[N]}}^{\pi} f_{\alpha\beta}(\theta)\theta^{-\alpha}\,|J_{\alpha+1}(N\theta)|\,d\theta \qquad (29)\\
&\quad + (2^{-\alpha}N^\alpha/\Gamma(\alpha+1))\sum_{k=1}^{[N]-1}(-1)^k\int_{\theta_k}^{\theta_{k+1}} f_{\alpha\beta}'(\theta)\theta^{-\alpha}J_\alpha(N\theta)\,d\theta \\
&\quad + O(n^{\alpha-\frac{1}{2}}) + O(n^{\alpha-\beta-1}),
\end{aligned}
$$

where $[N]$ denotes, as usual, the greatest integer $\leqq N$, and

$$
g_{\alpha\beta}(\theta) = 2^\alpha f_{\alpha\beta}(\theta)\theta^{-2\alpha}. \qquad (30)
$$

Now we need the asymptotic estimates

$$
\begin{cases} j_{\alpha+1,k} = (k+\frac{1}{2}\alpha+\frac{1}{4})\pi + O(k^{-1}); \\ M_k(\alpha) = (2/\pi)^{\frac{1}{2}} j_{\alpha+1,k}{}^{\alpha-\frac{1}{2}} + O(j_{\alpha+1,k}{}^{\alpha-\frac{3}{2}}), \end{cases} \qquad (31)
$$

the first of which follows from [11, p. 506], the second becoming then a consequence of [11, p. 488] or [10, p. 15, (1.71.7)].

Now, $J_{\alpha+1}(t) = O(t^{-\frac{1}{2}})$ and $\theta_{[N]} = \pi - O(n^{-1})$, so that

$$
N^\alpha \int_{\theta_{[N]}}^{\pi} f_{\alpha\beta}(\theta)\theta^{-\alpha}\,|J_{\alpha+1}(N\theta)|\,d\theta = O(n^{\alpha-1}), \qquad (32)
$$

since the left member is

$$
\begin{aligned}
O(n^{\alpha-\frac{1}{2}})\int_{\theta_{[N]}}^{\pi}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}\,d\theta &= O(n^{\alpha-\frac{1}{2}})\int_0^{O(1/n)}\theta^{\beta+\frac{1}{2}}\,d\theta \\
&= O(n^{\alpha-\beta-2}) = O(n^{\alpha-1}),
\end{aligned}
$$

since $\beta > -1$.

Furthermore,

$$
g_{\alpha\beta}(\theta_1)M_1(\alpha) = M_1(\alpha) + O(n^{-2}), \qquad (33)
$$

since $g_{\alpha\beta}(\theta)$ is an even analytic function assuming the value 1 at the origin and $\theta_1 = j_1/N$, while

$$
g_{\alpha\beta}(\theta_{[N]})M_{[N]}(\alpha) = O(n^{\alpha-\beta-1}), \qquad (34)
$$

a magnitude already included in the error in (29).

The estimate (34) follows from (30) and (31), since $\theta_{[N]} = \pi - O(n^{-1})$, while

$$g_{\alpha\beta}(\theta_{[N]})M_{[N]}(\alpha) = O(\{\cot\tfrac{1}{2}(\pi - n^{-1})\}^{\frac{1}{2}}\{\sin(1/n)\}^{\beta})O(n^{\alpha-\frac{1}{2}})$$
$$= O(n^{-\frac{1}{2}-\beta+\alpha-\frac{1}{2}}) = O(n^{\alpha-\beta-1}).$$

Next we consider

$$(35)\qquad D_n \equiv (N^{\alpha}/\Gamma(\alpha+1))\sum_{k=1}^{[N]-1}(-1)^k\int_{\theta_k}^{\theta_{k+1}} f_{\alpha\beta}'(\theta)\theta^{-\alpha}J_{\alpha}(N\theta)\,d\theta,$$

in the form

$$D_n = (N^{2\alpha-1}/\Gamma(\alpha+1))\sum_{k=1}^{[N]-1}(-1)^k\int_{j_k}^{j_{k+1}} f_{\alpha\beta}'(x/N)x^{-\alpha}J_{\alpha}(x)\,dx.$$

From (28) it is clear that $f_{\alpha\beta}(\theta)$ is $2^{-\alpha}\theta^{2\alpha}$ times an even analytic function, regular in a neighborhood of the origin, whose value at the origin is 1. Thus,

$$f_{\alpha\beta}(\theta) = 2^{-\alpha}\theta^{2\alpha}\{1 + O(\theta^2)\},\qquad (\theta\to 0),$$

whence

$$f_{\alpha\beta}'(\theta) = 2^{-\alpha}(2\alpha)\theta^{2\alpha-1} + O(\theta^{2\alpha+1}),\qquad (\theta\to 0).$$

Hence

$$D_n = (2^{-\alpha}/\Gamma(\alpha+1))\sum_{k=1}^{[N]-1}(-1)^k\int_{j_k}^{j_{k+1}}\{2\alpha + O(x^2/N^2)\}x^{\alpha-1}J_{\alpha}(x)\,dx.$$

The remainder term in this integrand contributes to D_n an amount which is

$$O(N^{-2})\sum_{k=1}^{[N]-1}\int_{j_k}^{j_{k+1}} x^{\alpha+1}\,|J_{\alpha}(x)|\,dx$$
$$= O(N^{-2})\int_{j_1}^{j_{[N]}} x^{\alpha+1}\,|J_{\alpha}(x)|\,dx$$
$$= O(N^{-2})\int_{j_1}^{j_{[N]}} x^{\alpha+\frac{1}{2}}\,dx = O(N^{-2})\,j_{\alpha+1,[N]}{}^{\alpha+\frac{3}{2}}$$
$$= O(N^{\alpha-\frac{1}{2}}) = O(n^{\alpha-\frac{1}{2}}),$$

since $J_{\alpha}(x) = O(x^{-\frac{1}{2}})$, and $j_{\alpha+1,[N]} = O(N)$ according to (31).

So,

$$D_n = (2^{1-\alpha}/\Gamma(\alpha+1))\sum_{k=1}^{[N]-1}(-1)^k\int_{j_k}^{j_{k+1}} x^{\alpha-1}J_{\alpha}(x)\,dx + O(n^{\alpha-\frac{1}{2}}).$$

Now,

$$\left| \int_{j_k}^{j_{k+1}} x^{\alpha-1} J_\alpha(x)\,dx \right| = O(1) \int_{j_k}^{j_{k+1}} x^{\alpha-\frac{3}{2}}\,dx$$
$$= O(1)\{ j_{\alpha+1,k+1}{}^{\alpha-\frac{1}{2}} - j_{\alpha+1,k}{}^{\alpha-\frac{1}{2}} \} = O(1)\{ (k+1)^{\alpha-\frac{1}{2}} - k^{\alpha-\frac{1}{2}} \}$$
$$= O(k^{\alpha-\frac{3}{2}}),$$

where we have used again that $J_\alpha(x) = O(x^{-\frac{1}{2}})$ and (31), and, for the final estimate, the mean-value theorem of the differential calculus.

Thus,

$$(36) \qquad D_n = (2^{1-\alpha}\alpha/\Gamma(\alpha+1)) \sum_{k=1}^{\infty} (-1)^k \int_{j_k}^{j_{k+1}} x^{\alpha-1} J_\alpha(x)\,dx + O(n^{\alpha-\frac{1}{2}}),$$

where the infinite series is absolutely convergent, since each term is $O(k^{\alpha-\frac{3}{2}})$ and $\alpha < \frac{1}{2}$.

There remains only to consider the first (finite) sum on the right in (29). For this purpose we write

$$2 \sum_{k=2}^{[N]-1} g_{\alpha\beta}(\theta_k) M_k(\alpha)$$
$$(37) \qquad = 2 \sum_{k=2}^{[N]-1} g_{\alpha\beta}(\theta_k) \{ M_k(\alpha) - (2^{\frac{1}{2}}/\pi^{\frac{1}{2}}) \int_{j_{k-1}}^{j_k} x^{\alpha-\frac{1}{2}}\,dx \}$$
$$+ (2/\pi)^{\frac{1}{2}} \sum_{k=2}^{[N]-1} \int_{j_{k-1}}^{j_k} g_{\alpha\beta}(\theta_k) x^{\alpha-\frac{1}{2}}\,dx.$$

Here we note that $g_{\alpha\beta}(\theta)$ is an even analytic function, regular in a neighborhood of the origin, which assumes the value 1 at the origin. Thus, from (31), $g_{\alpha\beta}(\theta_k) = 1 + O(k^2/n^2)$, $k = 2, \cdots, [N]-1$.

We consider first the contribution induced by the remainder $O(k^2/n^2)$ to the first sum in the right member of (37). In that sum, the expression in braces is $O(k^{\alpha-\frac{3}{2}})$, from (31), so that the contribution now under discussion is

$$O(n^{-2}) \sum_{k=2}^{[N]-1} k^2 k^{\alpha-\frac{3}{2}} = O(n^{-2}) \sum_{k=2}^{[N]-1} k^{\alpha+\frac{1}{2}} = O(n^{\alpha-\frac{1}{2}}).$$

Thus, $g_{\alpha\beta}(\theta_k)$ can be replaced in the first sum on the right in (37) by 1, with error $O(n^{\alpha-\frac{1}{2}})$, an amount which can be absorbed in the error terms already present in (29).

Passing to the final sum on the right of (37), we note that $g_{\alpha\beta}(\theta_k) = g_{\alpha\beta}(\theta) + O(n^{-1})$, as can be inferred from the mean-value theorem of differential calculus, since $g_{\alpha\beta}(\theta) = 1 + O(n^{-2})$ and $g_{\alpha\beta}'(\theta) = O(n^{-1})$. Re-

placing $g_{\alpha\beta}(\theta_k)$ by $g_{\alpha\beta}(\theta)+O(n^{-1})$, we find that the error term induces a contribution of

$$O(n^{-1})\sum_{k=2}^{[N]-1}\int_{j_{k-1}}^{j_k} x^{\alpha-\frac{1}{2}}\,dx = O(n^{-1})\int_{j_1}^{j_{[N]-1}} x^{\alpha-\frac{1}{2}}\,dx = O(n^{\alpha-\frac{1}{2}}),$$

since $j_{[N]}=O(N)=O(n)$ from (31).

Hence,

$$(38)\qquad \begin{aligned} 2\sum_{k=2}^{[N]-1} g_{\alpha\beta}(\theta_k)M_k(\alpha) &= 2\sum_{k=2}^{\infty}\{M_k(\alpha)-(2^{\frac{1}{2}}/\pi^{\frac{3}{2}})\int_{j_{k-1}}^{j_k} x^{\alpha-\frac{1}{2}}\,dx\} \\ &\quad + (2/\pi)^{\frac{3}{2}}\int_{j_1}^{j_{[N]-1}} g_{\alpha\beta}(\theta)x^{\alpha-\frac{1}{2}}\,dx + O(n^{\alpha-\frac{1}{2}}), \end{aligned}$$

where the passage from the finite sum which arises directly from our discussion of the first finite sum on the right of (37) to the (absolutely convergent) infinite series in (38) leads to an error of only $O(n^{\alpha-\frac{1}{2}})$ since each term of the series is $O(k^{\alpha-\frac{3}{2}})$ from (31).

Now, using (28) and (30) and putting $x=N\theta$,

$$\begin{aligned} &\int_{j_1}^{j_{[N]-1}} g_{\alpha\beta}(\theta)x^{\alpha-\frac{1}{2}}\,dx \\ &= 2^{\alpha-\frac{1}{2}}N^{\alpha+\frac{1}{2}}\int_{\theta_1}^{\theta_{[N]-1}}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}\,d\theta \\ &= 2^{\alpha-\frac{1}{2}}N^{\alpha+\frac{1}{2}}\int_{0}^{\pi}(\sin\tfrac{1}{2}\theta)^{\alpha-\frac{1}{2}}(\cos\tfrac{1}{2}\theta)^{\beta+\frac{1}{2}}\,d\theta + O(n^{\alpha-\frac{1}{2}}) \\ &= 2^{\alpha-\frac{1}{2}}N^{\alpha+\frac{1}{2}}\Gamma(\tfrac{1}{2}\alpha+\tfrac{1}{4})\Gamma(\tfrac{1}{2}\beta+\tfrac{3}{4})/\Gamma(\tfrac{1}{2}\{\alpha+\beta\}+1)+O(n^{\alpha-\frac{1}{2}}). \end{aligned}$$

The replacement of θ_1 and $\theta_{[N]-1}$ by 0 and π, respectively, introduces the stated error $O(n^{\alpha-\frac{1}{2}})$, since $\theta_1=O(n^{-1})$ and $\pi-\theta_{[N]-1}=O(n^{-1})$. The resulting integral is a standard form in the theory of the gamma and beta functions.

Now we substitute in (29) the above, together with (38), as well as (32), (33), (34), (35) and (36). This proves (2) with n replaced by N. Since $N-n$ is a constant, namely $\frac{1}{2}(\alpha+\beta+2)$, the error committed in replacing N by n in (2) is $O(n^{\alpha-\frac{1}{2}})$, an amount already present there.

This completes the proof of (2).

UNIVERSITY OF ALBERTA,
EDMONTON, ALBERTA, CANADA.

REFERENCES.

[1] T. H. Gronwall, "Über die Laplacesche Reihe," *Mathematische Annalen*, vol. 74 (1913), pp. 213-270.

[2] ———, "On the degree of convergence of Laplace series," *Transactions of the American Mathematical Society*, vol. 15 (1914), pp. 1-30.

[3] L. Lorch, "On Fejér's calculation of the Lebesgue constants," *Bulletin of the Calcutta Mathematical Society*, vol. 37 (1945), pp. 5-8.

[4] ———, "Asymptotic expressions for some integrals which include certain Lebesgue and Fejér constants," *Duke Mathematical Journal*, vol. 20 (1953), pp. 89-104.

[5] ———, "The Lebesgue constants for Jacobi series, I," *Proceedings of the American Mathematical Society*, vol. 10 (1959), pp. 756-761.

[6] H. Rau, "Über die Lebesgueschen Konstanten der Reihenentwicklungen nach Jacobischen Polynomen," *Journal für die reine und angewandte Mathematik*, vol. 161 (1929), pp. 237-254.

[7] G. Szegö, "Über einige asymptotische Entwicklungen der Legendreschen Funktionen," *Proceedings of the London Mathematical Society*, (2), vol. 36 (1932), pp. 427-450.

[8] ———, "Über eine von Herrn S. Bernstein herrührende Abschätzung der Legendreschen Polynome," *Mathematische Annalen*, vol. 108 (1933), pp. 360-369.

[9] ———, "Asymptotische Entwicklungen der Jacobischen Polynome," *Schriften der Königsberger Gelehrten Gesellschaft, naturwissensschaftliche Klasse*, vol. 10 (1933), pp. 35-112.

[10] ———, "Orthogonal polynomials," *Colloquium Publications of the American Mathematical Society*, vol. 23 (1939).

[11] G. N. Watson, *A treatise on the theory of Bessel functions*, 2d ed., Cambridge, 1944.

SELF-LINKED SUBGROUPS OF SEMIGROUPS.*

By M. L. Curtis.[1]

1. Introduction. A. D. Wallace posed the following question. If euclidean 3-space E^3 has a continuous associative multiplication with a unit, and C is a circle subgroup, does it follow that C is unknotted? The principal result of this note is that C is unknotted if it is tame. The hypothesis that there be a unit is not needed.

A set Y in a space S is said to be self-linked if Y is contractible to a point in S, but there does not exist a homotopy $\psi\colon Y \times I \to S$ such that:

(1) ψ^* is the identity,

(2) $\psi_t(Y) \subset S - Y$ for all $t > 0$,

(3) $\psi_1(Y)$ is a point.

We prove a basic theorem about compact self-linked subgroups of locally compact semigroups and use this result to prove that, in the situation of the first paragraph above, C cannot be self-linked.

Next we use a theorem proved by Papakyriakopoulos (and communicated to us by R. H. Fox) to the effect that if a tame simple closed curve in E^3 is not self-linked, then it is unknotted. (Some wild simple closed curves bound disks and hence are clearly not self-linked). The theorem is a slight generalization of Dehn's lemma.

2. Three trivial lemmas.

Lemma 1. *Let S be a semigroup, e be an idempotent in S, and $K = eSe$. If $x \in K$ has an inverse relative to e, then it has an inverse relative to e in K.*

Proof. Let $xy = e$ with $x \in K$. Then $x = eze$ so that $exe = eze$ and hence $x = exe$. Now $exey = e$ implies that $exeeye = e$, so that $eye \in K$ is also a right inverse for x relative to e.

We note for future reference that $K = eSe$ is precisely the set of all elements of S for which e acts as an identity.

* Received ——————————.

[1] Supported in part by National Science Foundation Grant G-4211.

LEMMA 2. *Let S be a semigroup and e an idempotent in S. Le*[redacted] *a subgroup of $K = eSe$ such that e is the identity of C. If $x \in$* [redacted] *$xC \cap C \neq \phi$ (or $Cx \cap C \neq \phi$), then $x \in C$.*

Proof. Suppose $xr = c$ with r and c in C. Then $xrr^{-1} = cr^{-1}$ so t[redacted] $xe = cr^{-1}$. Since e is an identity for x, we have $x = cr^{-1} \in C$.

LEMMA 3. *Let S be a topological semigroup with e, C, K as in Lemma 2. If $\alpha\colon I \to S$ is a path such that $\alpha(0) = e$ and $\alpha(t) \in K - C$ for each $t > 0$, then the homotopy $\phi\colon C \times I \to S$ defined by $\phi(c,t) = c\alpha(t)$ is such that ϕ_0 is the identity and $\phi(c,t) \in K - C$ for all $t > 0$.*

Proof. The only thing to prove is that $\phi(c,t) \in K - C$ for each $t > 0$. Suppose $c\alpha(t) = d$ with $c, d \in C$. Then $e\alpha(t) = c^{-1}d$ and $\alpha(t) \in K$, so Lemma 2 implies $\alpha(t) \in C$ contradicting an hypothesis.

3. Basic theorem.

THEOREM 1. *Let S be a locally compact topological semigroup with a compact self-linked subgroup C having identity e. Suppose that each point x of $K - C$ $(K = eSe)$ can be joined to e by a path α such that $\alpha(0) = e$ and $\alpha(t) \in K - C$ for all $t > 0$. Then K is a topological group.*

Proof. It follows from elementary group theory together with Lemma 1 that K is a group if each $x \in K$ has a right inverse relative to e (which is clearly an idempotent).

Since C is self linked there is a contraction $\pi\colon C \times I \to S$ of C to a point. Let $H = \pi(C \times I)$. We will show that for each $x \in K$, $xH \cap C \neq \phi$.

Choose a path α from e to x as in the hypotheses of the theorem.. Define a homotopy of C by

$$\theta(c,t) = \begin{cases} \alpha(2t)c & 0 \leqq t \leqq \frac{1}{2} \\ x\pi(c, 2t-1) & \frac{1}{2} \leqq t \leqq 1. \end{cases}$$

We see that $\theta(C,1)$ is a point. Also θ is well defined at $\frac{1}{2}$ because $\alpha(1)c = xc$ and $x\pi(c,0) = xc$. Since C is self-linked there must exist (c_0, t_0) such that $\theta(c_0, t_0) \in C$. By Lemma 3 we must have $t_0 > \frac{1}{2}$. Hence $x\pi(c_0, 2t_0 - 1) \in C$ and $xH \cap C \neq \phi$ as asserted.

Then for $x \in K$ we can choose $y \in H$ such that $xy \in C$. Then xy has an inverse m in C and $xym = e$. By Lemma 1 we have that $eyme$ is an element of K which acts as an inverse for x. Hence K is a group. To show that K is a topological group it remains to show that the inverse map is continuous.

Let $\rho\colon K \times H \to S$ be the multiplication of S cut down to $K \times H$. Let

${}^{-1}(C)$. Define $\beta: P \to S$ by $\beta(x,y) = y(xy)^{-1}$ and define $\phi: S \to S$ by $= eye$. For $x \in K$ let $L_x = [(x,y) \mid (x,y) \in P]$. Then the inverse map be described by

$$x \to L_x \xrightarrow{\beta} S \xrightarrow{\phi} K.$$

Hence for each x, $\phi\beta(L_x)$ is a point and clearly β and ϕ are continuous.

We note that since S is locally compact and ϕ is a retraction, K is locally compact. Since C is compact, H is compact. From this it follows that the set function mapping x to L_x is upper semicontinuous. Let x_0^{-1} be the inverse of x_0; i.e. $x_0^{-1} = \phi\beta(L_{x_0})$. Let U be a neighborhood of x_0^{-1}. Then there exists a neighborhood W of L_{x_0} in P such that $\phi\beta(W) \subset U$. Since the $x \to L_x$ mapping is upper semicontinuous, there exists a neighborhood V of x_0 such that for $x \in V$ we have $L_x \cap W \neq \phi$. It follows that $\phi\beta(L_x)$ lies in U for each x, establishing the continuity of the inverse map.

4. Application to E^3.

THEOREM 2. *If E^3 has a continuous associative multiplication and contains a circle subgroup C, then C cannot be self-linked.*

Proof. Assume that C is self-linked. Let e be the identity of C, and let $K = eE^3e$. We will show that K is a topological group, and by Theorem 1 this will follow if we can find paths α form e to points x in $K - C$ with only the end point of α in C.

Now K is arcwise connected since $\phi: E^3 \to K$ is a retraction. Given $x \in K - C$, let β be a path from some point c_0 of C to x such that for $t > 0$ we have $\beta(t) \in K - C$. Let θ be a path from c_0^{-1} to e in C. Define $\alpha(t) = \beta(t)\theta(t)$, and note that $\alpha(0) = \beta(0)\theta(0) = c_0c_0^{-1} = e$ and that $\alpha(1) = \beta(1)\theta(1) = xe = x$. Also if $t > 0$, then $a(t) = \beta(t)\theta(t)$ and $\theta(t) \in C$. If $\alpha(t) \in C$, then we would have a contradiction of our choice of β. Hence K is a topological group.

Now K is a closed subset of E^3. For if y is a limit point of K, then eye is a limit point of precisely the same subsets of K of which y is a limit point, since for each x in K we have that $x = exe$.

Next we show that K is 2-dimensional. Suppose that $\dim K = 3$. Then K contains an open set in E^3, and since it is homogeneous, K must be open. It follows that $K = E^3$. Then K is a Lie group with the compact subgroup C, and we have a fibering of E^3 with a compact fiber. This is not possible (see [1] and [3]) so that $\dim K < 3$. Now K is contractible since it is a

retract of a contractible space. Thus K contains a singular disk with C boundary, showing that $\dim K > 1$, so that $\dim K = 2$.

The existence of the retraction ϕ implies that K is locally contrac. It is clearly locally compact and finite dimensional, so it follows from theorem on page 185 of [2] that it is a Lie group. As a contractib. 2-dimensional Lie group K is a plane. Since $C \subset K$, C cannot be self-linked, and this contradiction establishes the theorem.

COROLLARY. *With the hypotheses of Theorem 2 if C is also tame, then C is unknotted.*

Proof. This follows immediately from Theorem 2 and the theorem of Papakyriakopoulos mentioned in the introduction.

UNIVERSITY OF GEORGIA.

REFERENCES.

[1] Borel-Serre, "Impossibilite de fibrer un espace eucliden par des fibres compactes," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, vol. 230 (1950), pp. 2258-2260.

[2] Montgomery-Zippin, *Topological transformation groups*, New York, 1955.

[3] Arnold Shapiro, "Cohomologie dan des espaces fibres," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, vol. 231 (1950), pp. 206-207.

ON INVOLUTIONS OF THE 3-SPHERE.*

By Morris W. Hirsch and Stephen Smale.[1]

1. Introduction. If T is an orientation reversing involution of the 3-sphere S^3, it follows from the Smith theory [15] that the fixed point set F of T is either a 2-sphere or two points. If F is a 2-sphere, it may be wildly embedded in S^3 [2], in which case T will not be equivalent to a linear involution. (If T_1 and T_2 are involutions on spaces X_1 and X_2 respectively, an *equivalence* between T_1 and T_2 is a homeomorphism $h\colon X_1 \to X_2$ such that $hT_1 = T_2h$.) On the other hand if $F = S^2$ is tamely embedded, it is easy to show that T is equivalent to a reflection through an equatorial 2-sphere of S^3. The main purpose of this paper is to study the case where F is two points. We will prove

Theorem 1.1. *If $T\colon S^3 \to S^3$ is an involution with fixed point set F consisting of two points, then T is equivalent to the linear involution: $L\colon S^3 \to S^3$, $L(x_1, x_2, x_3, x_4) = (x_1, -x_2, -x_3, -x_4)$.*

Here we suppose that S^3 is the unit sphere in Euclidean 4-space with coordinates (x_1, x_2, x_3, x_4). If T is differentiable, then one can obtain actually a differentiable equivalence by our methods.

Theorem 1.1 answers a question of Floyd [6, p. 92].

The problems concerning an orientation-preserving involution on S^3 remain largely unsolved.[2]

As a by-product of the proof of 1.1, the following two theorems are proved:

Theorem 1.2. *Let M be a non-orientable triangulated 3-manifold with an element β of $\pi_1(M)$ such that $\beta^2 = 1$ and β reverses orientation. Then the projective plane P can be embedded in M piecewise linearly.*

Theorem 1.3. *Let T be an involution on a topological 3-manifold M*.

* Received January 26, 1959.

[1] Both authors have been supported in this research by the National Science Foundation.

[2] For the 2-sphere these problems have been solved by Eilenberg and Kerekjarto; see S. Eilenberg, *Fund. Math.* XXII (1934), pp. 28-41.

with an isolated fixed point y_0 not in the boundary of M. Then there is an invariant Euclidean neighborhood V of y_0 such that T restricted to V is equivalent to a linear involution. Furthermore, suppose V is a Euclidean neighborhood of y_0 and $h\colon \partial V \to S^2 \subset E^3$ is an equivalence between $T \mid \partial V$ and $S \mid S^2$, the reflection through the origin of E^3. Then h can be extended to an equivalence between T and S.

The proofs of the above theorems depend strongly on the methods of Papakyriakopoulos [11], especially in the version of A. Shapiro and J. H. C. Whitehead [13].

2. **Proof of 1.2.** Let α be the generator of $\pi_1(P) \approx Z_2$. An *orientation reversing embedding* $f\colon P \to M$ is a one-one piecewise linear map such that $f_{\#}(\alpha)$ reverses orientation in M. The proof of 1.2 is similar to the proof of Dehn's lemma by Shapiro and Whitehead [13]. We shall prove the following statement, which implies 1.2:

2.1. There exists an orientation reversing embedding $f\colon P \to M$ if and only if there exists $\beta \in \pi_1(M)$ which reverses orientation, and such that $\beta^2 = 1$.

It is clear that given an orientation reversing embedding $f\colon P \to M$, then $\beta = f_{\#}(\alpha)$ reverses orientation (by definition) and $\beta^2 = 1$ because $\alpha^2 = 1$. It remains to find f, given β. It should be remarked that we do not prove that there exists an embedding $f\colon P \to M$ such that $f_{\#}(\alpha) = \beta$. The proof of 2.1 is broken up into several lemmas.

A map $f\colon P \to M$ is *canonical* if it is piecewise linear, maps each 2-simplex in a one-one fashion, and $f(P)$ has *double curves* and *triple points* (see [11, § 2]) as singularities.

To obtain canonical maps, it is convenient to use their differentiable analogues, *normal immersions*. We can assume M has a differentiable structure [5], which by [14] is unique up to diffeomorphism. A map $f\colon P \to M$ is an *immersion* if it is differentiable and has Jacobian of rank 2 everywhere. We say an immersion $f\colon P \to M$ is *normal* if whenever $x_1, \cdots, x_n$ are points of P such that $y = f(x_1) = \cdots = f(x_n)$, then the intersection of the n tangent planes to $f(P)$ at y has minimal dimension. It follows that $n \leq 3$, and that $f(P)$ has only double curves and triple points as singularities.

It is shown in [7] that if A and B are manifolds, $\dim A < \dim B$, and A can be immersed in B, then any map $A \to B$ can be approximated by an

immersion.[3] Since P can be immersed in Euclidean 3-space (Boy's surface) P can be immersed in any 3-manifold M. In [8] it is shown that any immersion can be approximated by a normal immersion. We leave it to the reader to prove that a normal immersion can be approximated by a canonical map. (Compare this statement with [4], for example). Using these approximations and the fact that every 3-manifold has a triangulation, unique up to subdivision [9], we have proved:

LEMMA 2.2. *Any map $f\colon P\to M$ can be approximated (and is thus homotopic to) a canonical map.*

LEMMA 2.3. *Let $\beta\in\pi_1(M)$ be such that $\beta^2=1$. There exists a canonical map $f\colon P\to M$ such that $f_\#(\alpha)=\beta$.*

Proof. Let D be the unit disc in the complex plane and S^1 its boundary. Let $\lambda\colon S^1\to M$ be a map representing β. Let $\mu\colon S^1\to S^1$ be the double covering $e^{i\theta}\to e^{2i\theta}$. Then $\lambda\mu\colon S^1\to M$ represents $\beta^2=1$, and is therefore extendable to a map $h\colon D\to M$. Since h sends antipodal points of S^1 into the same point, h defines a map $g\colon P\to M$, if we consider P to be obtained from D by identifying antipodal boundary points. It is clear that $g_\#(\alpha)=\beta$. By 2.2 there is a canonical map $f\colon P\to M$, homotopic to g. Thus $f_\#(\alpha)=\beta$, and 2.3 is proved.

Let $f\colon P\to M$ be a canonical map, and put $P_0=f(P)$. By a *regular neighborhood* of P_0 we mean a 3-manifold V (with boundary) such that V is a sub-complex of M containing P_0, and admitting P_0 as a deformation retract. It is easy to construct regular neighborhoods (cf. [13]).

Given f and V as above, we say a covering space $p\colon V'\to V$ is *proper* if it is two sheeted, and $f_\#(\alpha)\in p_\#(\pi_1(V'))$.

LEMMA 2.4. *Let V be a compact non-orientable 3-manifold with non-empty boundary ∂V. If $H_1(V)$ is finite, then at least one component of ∂V is a projective plane.*

Proof. We first show that not every component of ∂V is the boundary of a 3-manifold. This is because a compact 2-manifold N which bounds some 3-manifold bounds a (possibly non-orientable) *henkelkörper* Q, in the sense of [12]. The embedding $i\colon N\to Q$ has the property that $i_*\colon H_1(N)\to H_1(Q)$ is onto. Now suppose that each component N_i of ∂V bounds a *henkelkörper* Q_i. Then the union of V and the Q_i forms a compact non-orient-

[3] The map $A\to B$ must be homotopic to an immersion. Using the results in [7], it is easy to show that any map $P\to M$ has this property.

able 3-manifold W without boundary, and because $i_*: H_1(N_i) \to H_1(Q_i)$ is onto, and $H_1(V)$ is finite, it follows that $H_1(W)$ is finite, in contradiction to [12, Satz IV, p. 206].

Thus some component of ∂V is not a boundary, and therefore is non-orientable. Let there be $s \geqq 1$ non-orientable components X_i of ∂V, whose genera (number of cross-caps) are $k_1, \cdots, k_s$, and $r \geqq 0$ orientable components Y_j whose genera are $h_1, \cdots, h_r$, if $r > 0$. We must show that some $k_i = 1$.

The Betti numbers b_n of V satisfy $b_0 = 1$, $b_1 = 0$, $b_3 = 0$, and $b_2 \geqq r$; the last relation follows from the fact that $H^3(V, \partial V) = 0$, since V is non-orientable. Let χ stand for Euler characteristic; then [12, p. 223] $\chi(V) = 2\chi(\partial V)$. Substituting in this the values $\chi(X_i) = 2 - k_i$, $\chi(Y_j) = 2 - 2h_j$, and the relations among the b_n above, we obtain, after simplifying, $s \geqq \sum_1^r h_j + \frac{1}{2} \sum_1^s k_i + 1$. Since each $h_j \geqq 0$ and each $k_i \geqq 1$, it follows that some $k_i = 1$. This prove 2. 4.

LEMMA 2. 5. *Let $f: P \to M$ be a canonical map and V a non-orientable regular neighborhood of $f(P)$. If V has no proper cover, then there is an orientation reversing embedding of P in V.*

Proof. The boundary ∂V of V consists of a finite number of compact 2-manifolds. We shall show that some component of ∂V is a projective plane. Let $\psi: \pi_1(V) \to H_1(V)$ be the Hurewicz homomorphism. If $H_1(V)$ were infinite, we could map $H_1(V)$ onto Z_2 such that $\psi f_\#(\alpha)$ would be in the kernel K; the covering of V corresponding to $\psi^{-1}(K)$ would then be proper, contrary to hypothesis. Therefore $H_1(V)$ is finite. By 2. 4, ∂V contains a projective plane P' which is piecewise linearly embedded in M. It is clear that the embedding $P' \to V$ reverses orientation in V, and therefore also in M, and 2. 5 is proved.

LEMMA 2. 6. *Let $f: P \to V'$ be an orientation reversing embedding, and let $p: V' \to V$ be a double covering. There exists an orientation reversing embedding $P \to V$.*

Proof. Let $g = pf: P \to V$. By a slight deformation of f, keeping it an embedding, we may assume that g is a canonical map. Clearly, $g_\#(\alpha)$ reverses orientation in V, since $f_\#(\alpha)$ does so in V'. Since f is one-one and p is two-one, $g(P)$ has no triple points, but only double curves as self-intersections and these consist of mutually disjoint simple closed curves, piecewise linearly embedded in $g(P)$. Let C be such a double curve. Then $g^{-1}(C)$ consists of a pair (not necessarily distinct) of simple closed curves C', C'' contained in P. There are several cases to consider:

i) $C' = C''$, C' homotopically trivial
ii) $C' = C''$, C' not homotopically trivial
iii) $C' \neq C''$, both homotopically trivial
iv) $C' \neq C''$, one (say C') not homotopically trivial.

Case i) cannot occur, for both C' and C, being null-homoptopic, preserve orientation, but it is easily seen that C must reverse orientation if $C'' = C'$ (cf. [8, 3.1]). *Case* ii) is impossible, for $C' = C''$ means the map $g\colon C' \to C$ is a double covering, hence the homotopy class $g_{\#}(\alpha)$ can be represented as β^2, where β is the homotopy class of C (with some orientation). But $g_{\#}(\alpha)$ reverses orientation, while the square of any homotopy class preserves orientation. *Case* iii) In this situation C' and C'' bound discs and the original "cuts" (*umschaltungen*) of Dehn can be used, as described e.g. in [11]. It is easy to check that after making the cuts, the map $g_1\colon P \to V$ is canonical, has no triple points, fewer double curves than g, and $g_{1\#}(\alpha)$ reverses orientation. *Case* iv) is impossible, for $g_{\#}(\alpha) \neq 1$ (because it reverses orientation), and if C' represents α, C'' must also; but on a projective plane any two non-null-homotopic curves must intersect, contradicting the result that C' and C'' are disjoint. Thus all pairs C', C'' are as in *Case* iii), and by making a finite number of cuts, we obtain an orientation reversing embedding of P in V.

Proof of 2.1. By 2.3, there is a canonical map $g\colon P \to M$, such that $g_{\#}(\alpha) = \beta$, β reversing orientation. Let V be a regular neighborhood of $g(P)$. If V has no proper cover, then 2.5 implies 2.1. Otherwise let $p\colon V' \to V$ be a proper cover. Since $g_{\#}(\alpha) \in p_{\#}\pi_1(V')$ by the definition of proper cover, there is a map $g'\colon P \to V'$ such that $pg' = g$. It is clear that g' is canonical and $g'_{\#}(\alpha)$ reverses orientation. Moreover, it is easily seen, as in [11, 9.1], that $g'(P)$ has fewer curves than $g(P)$. If $g'$is an embedding, 2.1 follows from 2.6. If not, we take a regular neighborhood V'' of P', a proper cover of V'' (if possible; if not, 2.1 follows from 2.5 and 2.6), and proceed inductively. Thus 2.1 is proved by 2.5, 2.6, and induction on the number of double curves of $g(P)$.

Remarks. Concerning the problem of embeddings $f\colon P \to M$ such that $f_{\#}(\alpha)$ preserves orientation, we have the following results, which are not used in the rest of the paper.

2.7. If there exists an embedding $f\colon P \to M$ such that $f_{\#}(\alpha)$ preserves orientation, then Z_2 is a free factor of $\pi_1(M)$.

Proof. Let V be a regular neighborhood of $f(P)$, where f is as in 2.6. Then $\chi(V) = \chi(f(P)) = 1$, since $f(P)$ is a deformation retract of V. Since

$2\chi(V) = \chi(\partial V)$, we have $\chi(\partial V) = 2$. Since each component of ∂V is orientable, ∂V is a 2-sphere Σ, which separates M into two parts, whose closures are V and V_1 (say), with $V \cap V_1 = \Sigma$. It follows that $\pi_1(M)$ is the free product of $\pi_1(V_1)$ and $\pi_1(V) \approx Z_2$.

In the case where f is assumed to be a *differentiable embedding*, we can choose for V a "tubular" neighborhood of $f(V)$. In this case it is easily seen, by considering the normal bundle of $f(P)$, that V is homeomorphic to the mapping cylinder of the double covering $S^2 \to P$. This proves:

2.8. A necessary and sufficient condition that there exist a differentiable embedding $f\colon P \to M$ such that $f_\#(\alpha)$ preserves orientation, is that M be the sum (in the sense of [12, p. 218]) of projective 3-space and another 3-manifold.

3. **Proof of 1.3.** We will use the following lemma.

LEMMA 3.1. *Let $R\colon S^2 \times I \to S^2 \times I$ be an involution without fixed points such that for $i = 0, 1, R(S^2 \times i) = S^2 \times i$ and R restricted to $S^2 \times i$ is equivalent to the antipodal map A on S^2. Then R is equivalent to $A \times e\colon S^2 \times I \to S^2 \times I$, where $e\colon I \to I$ is the identity. Furthermore, an equivalence between R and $A \times e$ on $S^2 \times 0$ can be extended to an equivalence on $S^2 \times I$.*

Proof. The orbit space $S^2 \times I \,|\, R = X$ is triangulable by Moise [9], and hence there is an induced triangulation on $S^2 \times I$ in which T is simplicial. In the rest of this section objects (maps, embeddings, etc.) will be considered from the piecewise linear point of view. Let $p\colon S^2 \times I \to X$ be the orbit map and let $X_i = p(S^2 \times i)$, $i = 0, 1$. It is well known [2] that an involution on S^2 without fixed points is equivalent to the antipodal map. Hence the X_i are homeomorphic to the projective plane.

We define a map of the cylinder $J = S^1 \times I$ into X as follows: Let $f_i\colon S^1 \times i \to X_i$, $i = 0, 1$, be embeddings which represent the non-trivial elements of $\pi_1(X_i)$. By consideration of the covering space maps $(S^2 \times i, p, X_i) \to (S^2 \times I, p, X)$, $i = 0, 1$, it is easily seen that f_0 and f_1 are homotopic in X. Thus we obtain a map $F\colon J \to X$ which is an extension of $f_0 + f_1$.

Since the boundary ∂J of J is embedded in ∂X, we can deform F slightly to a map $F'\colon J \to X$ such that if $J_0 = F'(J)$ and $\partial J_0 = F'(\partial J)$, then there are no self-intersections in a neighborhood of ∂J_0 and $\partial J_0 \subset \partial X$. Then J_0 is a Dehn surface of type $(0, 2)$ in the terminology of [13]. Application of [13, 1.1] yields an embedding $G\colon J \to X$ which agrees with F' on a neighborhood of ∂J. (Note that 1.1 of [13] first yields a non-singular surface of type $(0, q)$, $0 < q \leqq 2$, but in our case q must equal 2 since our boundary circles are essential.)

Denote $G(J)$ by J_1 and $p^{-1}(J_1)$ by Q. Since G is essential in X, Q will be a cylinder in $S^2 \times I$ which doubly covers J_1 and $\partial Q \subset \partial(S^2 \times I)$. Furthermore Q remains invariant under R.

Let $h\colon S^2 \times 0 \to S^2 \times 0$ be an equivalence between R and $A \times e$, both restricted to $S^2 \times 0$, and let $K = h(Q \cap S^2 \times 0)$. Let

$$Q_0 = \{(x, y) \in S^2 \times I \mid x \in K\}.$$

Then Q_0 is invariant under $A \times e$. By the well known analogue of 3.1 in dimension 2, h can be extended to an equivalence of R and $A \times e$ on Q and Q_0. Thus we have $h\colon (S^2 \times 0) \cup Q \to (S^2 \times 0) \cup Q_0$. Let the components of $S^2 \times I - Q$ be denoted by A and B, the components of $S^2 \times I - Q_0$ by A_0 and B_0. Then it follows from Newman's [10] and Alexander's [1] theorems that A, B, A_0, and B_0 are 3-cells. Extend h to a homeomorphism between A and A. Finally define h on B to be $(A \times e)hR$. This h is our desired equivalence between R and $A \times e$.

We now start the proof of 1.3. As before we can assume without loss of generality that T restricted to the complement of the fixed point set is piecewise linear. The following lemma is where 1.2 is used.

LEMMA 3.2. *In every neighborhood of y_0 there is an invariant 2-sphere.*

Proof of 3.2. Let U be a given Euclidean neighborhood of y_0 in M. Choose V to be an open connected neighborhood of y_0 such that $V \subset U$ and $TV \subset U$. Let $\pi\colon M \to M/T$ be the orbit may, $V^* = \pi(V)$, and $V_0 = V^* - \pi(y_0)$. We claim that V_0 satisfies the conditions of 1.2. From [3] it follows that T is orientation reversing, so V_0 is non-orientable. Let $x \in V$, $x \neq y_0$, and let $b(t)$ be an arc joining x to Tx in $(V \cup TV) - y_0$. Then it is easy to see that $\beta = \{\pi b(t)\}$ satisfies the conditions of 1.2. Hence there is an embedding $j\colon P \to V_0$ of the projective plane in V_0. The inverse image $\pi^{-1}(j(P)) \subset U$ will be the desired 2-sphere. This proves 3.2.

Returning to the proof of 1.3, let U be as in 3.2. If N is an embedded 2-sphere in U, denote by $C(N)$ the closure of the component of $M - N$ containing y_0. Then by 3.2 choose disjoint invariant 2-sphere $V_1, V_2, V_3, \cdots$ such that $\lim(\text{diameter } V_i) = 0$, $U \supset V_1$ and for each i, $C(V_i) \supset V_{i+1}$.

Let W_i be the sphere about the origin in E^3 of radius $1/i$ and let T_0 be the reflection through the origin of E^3. Let $h\colon V_1 \to W_1$ be some equivalence between the restrictions of T and T_0. By 3.1 extend h to

$$C(V_1) - \text{interior } C(V_2) \to C(W_1) - \text{interior } C(W_2).$$

Here we again use Newman's and Alexander's theorems to show that

$C(V_1)$ — interior $C(V_2)$ is homeomorphic to $S^2 \times I$. Repeated applications of 3.1 yield the desired equivalence of 1.3.

4. Proof of 1.1. Let the fixed points of T be denoted by y_1 and y_2. By 3.2 let V_1 and V_2 be disjoint invariant 2-spheres about y_1 and y_2 respectively. In S^3 let $W_1 = \{x \in S^3 \mid x_1 = \frac{1}{2}\}$ and $W_2 = \{x \in S^3 \mid x_1 = -\frac{1}{2}\}$. Let $h\colon V_1 \to W_1$ be an equivalence between the restrictions of T and L. By 3.1, extend h to be an equivalence on the domain of $S^3 - V_1 - V_2$ not containing the fixed points. Then by 1.3 h can be extended to an equivalence on all of S^3.

REFERENCES.

[1] J. W. Alexander, "On the subdivision of 3-space by a polyhedron," *Proceedings of the National Academy of Sciences U.S.A.*, vol. 9 (1923), pp. 6-8.

[2] R. H. Bing, "A homeomorphism between the 3-sphere and the sum of two solid horned spheres," *Annals of Mathematics*, vol. 56 (1952), pp. 354-362.

[3] G. Bredon, "Orientation in generalized manifolds and application to the theory of transformation groups," to appear.

[4] S. S. Cairns, "Polyhedral approximations to regular loci," *Annals of Mathematics*, vol. 37 (1936), pp. 409-415.

[5] ———, "Homeomorphism between topological and analytical manifolds," *ibid.*, vol. 41 (1940), pp. 796-808.

[6] E. E. Floyd, *Summary of Lectures and Seminars of Summer Institute on Set Theoretic Topology*, Madison, Wisconsin, 1955, pp. 92-96.

[7] M. W. Hirsch, *Immersions of manifolds*, Thesis, University of Chicago, 1958, to appear in *Transactions of the American Mathematical Society*.

[8] R. K. Lashof and S. Smale, "Self-intersections of an immersed manifold," to appear in *Journal of Mathematics and Mechanics*.

[9] E. E. Moise, "Affine structures in 3-manifolds, V. The triangulation theorem and hauptvermutung," *Annals of Mathematics*, vol. 56 (1952), pp. 96-114.

[10] M. H. A. Newman, "On the foundations of Combinatory Analysis Situs," *Proceedings of the Royal Academy of Amsterdam*, vol. 29, pp. 610-641.

[11] C. D. Papakyriakopoulos, "On Dehn's lemma and the asphericity of knots," *Annals of Mathematics*, vol. 66 (1957), pp. 1-26.

[12] H. Seifert and W. Trelfall, *Lehrbuch der Topologie*, New York, 1947.

[13] A. Shapiro and J. H. C. Whitehead, "A proof and extension of Dehn's Lemma," *Bulletin of the American Mathematical Society*, vol. 64 (1958), pp. 174-178.

[14] S. Smale, "On diffeomorphisms of the 3-sphere," to appear.

[15] P. A. Smith, Fixed points of periodic transformations, Appendix B in Lefschetz, *Algebraic Topology*, New York.

ON SPHERICAL IMAGE MAPS WHOSE JACOBIANS DO NOT CHANGE SIGN.*

By PHILIP HARTMAN and LOUIS NIRENBERG.[1]

Introduction. This paper is concerned with oriented hypersurfaces, of class C^2, of dimension n immersed in $(n+1)$-dimensional real Euclidean space E^{n+1} and with the property that the Jacobian of the spherical image mapping does not change sign. In case $n=2$, this means that the Gauss curvature does not change sign. The main result (Theorem II′) asserts that the spherical image map of a compact portion of the surface is monotone,[2] in the sense that the boundary of the image set is contained in the image of the boundary.

We shall deal mainly with hypersurfaces having simple projection on a hyperplane, i.e., admitting the representation $x^{n+1}=z(x^1,\cdots,x^n)$. The spherical image may then be adequately described in terms of the vector $p(x)=\operatorname{grad} z(x)$, where $x=(x^1,\cdots,x^n)$.

Thus a large part of the paper is concerned with mappings $p=p(x)$ of an n-dimensional x region D into n-dimensional p space, which are of class C^1 in D, of class C^0 in the closure $\bar{D}$, have the property that the vector $p(x)$ is locally a gradient (i.e., the Pfaffian $w=\sum p_k\,dx^k$ is closed, $dw=0$) and that the Jacobian of p with respect to x does not change sign. Our main result (Theorem II) asserts again that the boundary of the image of D is contained in the image $p(D')$ of the boundary D' of D.

Theorem II implies, in particular, that each component of $p(x)$ satisfies a weak maximum and minimum principle. This fact is used in Section 7

* Received January 29, 1959.

[1] The work of Hartman was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command under contract No. AF 18(603)-41, that of Nirenberg by the Office of Naval Research under contract ONR-N6-ORI-201(01). Reproduction in whole or in part is permitted for any purpose of the United States Government.

Nirenberg is a fellow of the A. P. Sloan Foundation.

[2] Our use of the word "montone" is derived from Lebesgue's notion [Rendiconti del Circolo Matematico di Palermo, vol. 24 (1907), p. 380] of a monotone function of two real variables. "Monotone" maps in our sense are "quasi-interior" in the sense of Whyburn [Memoirs of the American Mathematical Society, no. 1 (1950)], rather than "monotone" in his sense.

to derive an analogue of Rado's theorem [8] (see also von Neumann [6]) on saddle surfaces for n-dimensional hypersurfaces.

The basic lemmas used in proving Theorem II are given in Sections 2 and 3. In Section 3, we consider maps $p(x)$ of the type described above, which have a vanishing Jacobian. For such a mapping it is shown (Theorem I) that $p(D)$ is contained in $p(D')$. The proof depends on a sharpened form and a generalization of a standard theorem on the differential geometry of torses. Theorems II and II′ are presented in Sections 4 and 5.

On the basis of Lemma 2 and its corollaries, it is shown (Theorem III in Section 6) that a complete hypersurface of constant zero curvature in $(n+1)$-(Euclidean) space is an $(n-1)$-cylinder, i. e., the hypersurface is a cylinder erected over a curve. In particular, a complete 2-surface in 3-space having zero Gaussian curvature is a cylinder; cf. Pogorelov [7].

Sections 8 and 9 which form Part II of the paper are concerned with a more detailed study of surfaces, $n=2$, having zero Gauss curvature. Consider such a surface in (x^1, x^2, x^3) space with simple projection on the (x^1, x^2) plane, i. e., which admits a representation $x^3 = z(x^1, x^2)$ on, say, a bounded convex region D in the (x^1, x^2) plane. If $x = (x^1, x^2)$ in D is the limit of points in D corresponding to nonplanar points on the surface, then, as follows from the results of Section 3 (see Section 9), through x there is a unique straight line with endpoints on the boundary of D along which the normal to the surface (or grad z) is constant. In general this will not be true for a point having a neighborhood consisting entirely of planar points. Consider the following:

Example. Let D_1 be any convex subset of D closed relative to D with boundary consisting of a subset of D' and of straight line segments with endpoints on D'. In D, define the surface as follows: $z \equiv 0$ in D_1, and the surface is a cylinder in each connected component of $D - D_1$.

Thus, in general, through a point x in D_1 there is no line segment having the properties above. However, as we prove in Section 9 (Theorem B), there always exist rays from x, going to the boundary, and along which the surface normal is constant. In Theorem A of Section 9, we also describe in general the connected subsets D_1 of a domain D which are such that the normal to the surface may be constant there.

Part I.

1. Notation. In the following, unless otherwise stated $x = (x^1, \cdots, x^n)$, $p = (p_1, \cdots, p_n)$, $q = (q^1, \cdots, q^n)$ are n vectors, D is a domain (i. e., an

open connected set, which is sometimes assumed to be bounded) in x space, and D' is its boundary. By a k-dimensional plane section π_k of D through a point x of D is meant the connected component, containing x, of the intersection of D and a k-dimensional plane through x.

Let $p = p(x)$ be of class C^1 in D. Let $J(x)$ denote the Jacobian matrix $(\partial p_i/\partial x^k)$ (so that the Jacobian itself is $\det J(x)$); $r(x)$ the rank of $J(x)$; finally $r^*(x)$ the largest integer s with the property that every neighborhood of x contains a point x^* with $r(x^*) = s$. In particular, $r(x) \leqq r^*(x)$. Let S_k denote the subset of D defined by $r^*(x) \leqq k (\leqq n)$, so that S_k is an open set.

By a gradient mapping $p = p(x)$ in D will be meant a vector valued function which is of class C^1 in D and is such that the Pfaffian

$$w = \sum p_i \, dx^i \tag{1}$$

is closed,

$$dw = 0. \tag{2}$$

Since $p = p(x)$ is of class C^1, the requirement (2) is equivalent to the condition that $J(x)$ be a symmetric matrix.

All mappings $p = p(x)$ are of class C^1 in D and, in some cases, are also assumed to be of class C^0 in the closure $\bar{D} = D \cup D'$ of D.

The image of a set A will be abbreviated by $p(A)$, its boundary by $p'(A)$.

2. Maps with Jacobian not changing sign. The mappings $p = p(x)$ in this section are defined, and of class C^1, in a bounded domain D; they are also of class C^0 in $\bar{D}$. They are *not* assumed to be gradient mappings.

LEMMA 1. *Let $p = p(x)$ be a mapping with Jacobian not changing sign. Suppose that A is a sub-domain of D satisfying*

$$p(A) \cap p(D') = 0 \text{ and } p(A) \cap p'(D) \neq 0. \tag{3}$$

Then the Jacobian $\det J$ *is identically zero in A.*

In the particular case that $D = A$, condition (3) is equivalent to

$$p(D) \cap p(D') = 0 \text{ and } p'(D) \not\subset p(D'). \tag{3'}$$

Actually, this particular case implies the general case of the lemma.

The proof of the lemma, which depends on a theorem of K. Knopp and R. Schmidt [5], was suggested by the proof of A. Douglis for the maximum principle in [3].

Proof. Since the degree of the mapping is constant on each component of the complement of $p(D')$, the first part of (3) shows that the degree of

mapping d at each point in $p(A)$ is the same; and because of the second condition there is a point $x_0 \in A$ such that $p(x_0)$ is contained in $p'(D)$ but not in $p(D')$, so that the degree of mapping at $p(x_0)$ is zero. Hence $d = 0$.

Suppose now $\det J(y) \neq 0$, say, $\det J(y) > 0$ for some point y in A. The mapping $p = p(x)$ then maps a neighborhood U of y onto a full neighborhood $p(U)$ of $p(y)$. Since the p image of the x set where $\det J(x) = 0$ is an n-dimensional zero set (Knopp-Schmidt [5]; cf. also [9]), the neighborhood $p(U)$ contains points p^* such that $\det J(x) > 0$ at every preimage of p^*. Since p^* has no preimage on D' if $U \subset A$, it has only a finite number k of preimages in D. Hence the degree d of the mapping at p^* is $k > 0$. Contradiction!

The proof of Lemma 1 yields a more general result [3] where we replace the x and p spaces by n-dimensional manifolds.

LEMMA 1'. *Let M_1, M_2 be two n-dimensional orientable manifolds of class C^2. Let M be an open connected subset of M_1 with boundary M' and compact closure $\bar{M}$. Let N be a mapping of $\bar{M}$ into M_2 which is of class C^1 in M and C^0 in $\bar{M}$. Assume, having fixed some orientations, that the Jacobian of the mapping N does not change sign. Suppose further that*

$$N(M) \cap N(M') = 0 \text{ and } N'(M) \not\subset N(M').$$

Then the Jacobian of the mapping N is identically zero.

In the remainder of this section, we present some corollaries of Lemma 1 which are not used in the rest of the paper.

COROLLARY 1. *Let D and $p = p(x)$ be as in Lemma 1. Let $v = v(p)$ be a continuous mapping of the p space E^n into a v space E^m and let $v = v(p)$ be monotone in the sense that $v'(P) \subset v(P')$ holds for every bounded domain P in p space. (E.g., let $m = n$ and $v \equiv p$ or let $m = 1$ and $v = p_1$). Let V be a closed, bounded set containing $v(p(D'))$ and having a connected complement; e.g., let V be the convex hull of $v(p(D'))$. If, for a point x_0 of D, $v(p(x_0)) \notin V$, then $\det J(x_0) = 0$. If $v = v(p)$ takes p sets of measure zero into v sets of measure zero, then $\operatorname{vol} V \geqq \operatorname{vol} v(p(D))$.*

By $\operatorname{vol} A$ is meant the m-dimensional Lebesgue measure of the (simply covered, measurable) set A in v space.

---

[3] We have learned that, since this paper was completed, theorems similar to Lemma 1' have also been obtained by S. S. Chern, for $n = 2$, in "Complex analytic mappings of Riemann surfaces, I" to appear in this Journal and by S. Sternberg and R. G. Swan, for arbitrary n, in "On maps with non-negative Jacobian" to appear in the Michigan Mathematical Journal.

Remark. If $d = \operatorname{diam} v(p(D'))$ is the diameter of the set $v(p(D'))$, each of the two parts of the corollary furnishes a lower bound for d. Let V be the convex hull of $v(p(D'))$, so that $\operatorname{diam} V = d$. Let A be the open (possibly empty) subset of D where $\det J(x) \neq 0$, then by the first part, $v(p(A)) \subset V$; hence $d \geqq \operatorname{diam} v(p(A))$. When the conditions of the second part of the corollary hold, then $d \geqq 2(\operatorname{vol} v(p(D))/\omega_m)^{1/m}$, where ω_m is the volume of the m dimensional unit sphere $|v| < 1$. This inequality for d follows from a theorem of Bieberbach [1] which states that $\operatorname{vol} V \leqq \omega_m (d/2)^m$ when $d = \operatorname{diam} V$.

The inequality $d \geqq 2(\operatorname{vol} v(p(D))/\omega_m)^{1/m}$ generalizes a result of G. S. Young [11].

Proof of Corollary 1. Let $x_0 \in D$ and $v(p(x_0)) \notin V$. Suppose, if possible, that $\det J(x_0) \neq 0$. Let A be the connected component, containing x_0, of the set of points y in D such that $v(p(y)) \notin V$. Clearly, $v(p(A')) \subset V$, so that $p(A) \cap p(A') = 0$.

Since $\det J(x_0) \neq 0$, $p(x_0)$ is an interior point of $p(A)$. Let P be the connected component, containing $p(x_0)$, of the set of interior points p of $p(A)$. Since V is closed, bounded and has a connected complement, the point $v(p(x_0))$ can be joined to infinity in $E^m - V$, so that the boundary $v'(P)$ of the set $v(P)$ containing $v(p(x_0))$ is not contained in V. From the monotony of the mapping $v = v(p)$, it follows that $v'(P) \subset v(P')$, hence $v(P')$ is not contained in V. Finally, $v(P') \subset v(p'(A))$ and so, $v(p'(A))$ is not contained in V.

Hence $p(A) \cap p(A') = 0$ and $p'(A) \not\subset p(A')$. Consequently, Lemma 1 implies that $\det J$ vanishes in A, in particular, at x_0.

To prove the last part, suppose that $v(p(D)) - V$ has positive measure. Then, by our hypothesis on $v = v(p)$, the set of points $p(x)$ such that $v(p(x)) \notin V$ is not a zero set in p space. The theorem of Knopp-Schmidt [5] mentioned above implies that there is a point x with $\det J(x) \neq 0$ and $v(p(x)) \notin V$. This contradicts the first part of the corollary.

COROLLARY 2. *Let D and $p = p(x)$ be as in Lemma* 1. *Let $F(p)$ be real-valued, continuous function defined on p space and satisfying a weak maximum principle on every bounded domain (i.e., the maximum of F on the closure of the domain occurs on the boundary). Let $M = \max F(p(x))$ for $x \in D'$. If, for a point x_0 of D, $F(p(x_0)) > M$, then* $\det J(x_0) = 0$.

Proof. Clearly, $p(x_0) \notin p(D')$. Let A be the connected component, containing x_0, of the set of points y in D such that $F(p(y)) > M$. Then $F(p(x)) \leqq M$ on A', so that $p(A) \cap p(A') = 0$. Since the maximum of $F(p)$

on the boundary of every bounded p domain containing $p(A)$ is at least $F(p(x_0)) > M$, it follows that the maximum of $F(p)$ on $p'(A)$ exceeds M, so that $p'(A) \not\subset p(A')$. Consequently, by Lemma 1, $\det J \equiv 0$ on A; in particular, $\det J(x_0) = 0$.

As a consequence of Corollary 2, we have the following result of Liouville type.

COROLLARY 3. *Let $p = p(x)$ be a mapping of class C^1 of a domain D (possibly unbounded) into E^n, with Jacobian not changing sign. Suppose that there exists a non-negative, continuous function $F(p)$ defined on p space such that* (i) *$F(p)$ satisfies a weak maximum principle on every bounded domain,* (ii) *$F(p) \not\equiv 0$ on any open p set, and* (iii) *$F(p(x))$ tends to* 0 *as x tends to the boundary of D (or infinity). Then the Jacobian of the mapping $p(x)$ is identically zero.*

This is a more general form of a result stated in a note [11] by G. S. Young. There $D = E^n$ and it is assumed that $p(x)$ tends to a limit as $|x| \to \infty$. Corollary 3, with the choice $F(p) = |p_1 - \text{const.}|$, shows that it is sufficient to require, for example, that $p_1(x)$ tends to a limit as x tends to D'.

Note that condition (iii) can be relaxed to: (iii′) there exists a sequence $D_1, D_2, \cdots$ of bounded subdomains of D such that $\bar{D}_k \subset D_{k+1}$, $D = \cup D_k$, and $m_k = \max F(p(x))$ for $x \in D_k'$ satisfies $m_k \to 0$ as $k \to \infty$.

Proof. Let x be a point where $F(p(x)) > 0$. Denote by D_x the connected component, containing x, of points y with $F(p(y)) > \frac{1}{2}F(p(x))$. By condition (iii) on F, D_x is a bounded domain and $\bar{D}_x \subset D$. By condition (i) on F, Corollary 2 is applicable on D_x, so that $\det J \equiv 0$ there; in particular, $\det J = 0$ at x. Thus the Jacobian vanishes at all points x for which $F(p(x)) > 0$.

Suppose finally that $\det J \neq 0$ at a point x where $F(p(x)) = 0$. Then $p = p(x)$ maps a neighborhood U of x onto a neighborhood $p(U)$ of $p(x)$. Since $F(p) \not\equiv 0$ for $p \in p(U)$, it follows that there is a point $y \in U$ at which $F(p(y)) > 0$, so that $\det J(y) = 0$. Since this is true for some y in every sufficiently small U, the continuity of $\det J$ implies $\det J(x) = 0$.

3. Gradient maps with zero Jacobian. Throughout the section, we consider only gradient maps, with Jacobian identically zero, of class C^1 in a domain (which may be unbounded unless otherwise stated).

LEMMA 2. *Let $p = p(x)$ be a gradient mapping with Jacobian which is identically* 0. *If at a point x_0 of D, $r(x_0)$ and $r^*(x_0)$ have a common value k,*

then $p(x)$ is constant on an $(n-k)$-dimensional plane section $\pi_{n-k}(x_0)$ of S_k through x_0. Furthermore, all points x near x_0 for which $p(x)=p(x_0)$ lie on π_{n-k}. Finally, $r(x)=r^*(x)=k$ for all x on π_{n-k}.

Lemma 2 is essentially a result proved by Chern and Lashof; [2], Lemma 2, p. 314. A proof of Lemma 2 is given below.

An immediate consequence of Lemma 2 is the following.

COROLLARY 1. *If $r^*(x_0)=k$ at a point x_0 of D, then $p(x)$ is constant on an $(n-k)$-dimensional plane section π_{n-k} of S_k through x_0. Also $x\in\pi_{n-k}$ implies that $r^*(x)=k$ and that either $r(x)=k$ or $r(x)<k$ according as $r(x_0)=k$ or $r(x_0)<k$.*

The first assertion of the corollary follows from that of Lemma 2 by considering a sequence of points $x_1, x_2, \cdots$ tending to x_0 such that $r^*(x_j) = r(x_j)=k$ and that $\pi_{n-k}(x_j)$ tends to a limiting position containing a section π_{n-k} as $j\to\infty$. The second assertion of the corollary follows from the last part of Lemma 2.

Note that if $p=\operatorname{grad} z$, then z is clearly a linear function on π_{n-k} (in both Lemma 2 and Corollary 1).

In general one cannot assert the uniqueness of π_{n-k} in Corollary 1. Uniqueness does hold in the following simple case.

COROLLARY 2. *If $k=1$ in Corollary 1, then the plane section π_{n-1} of S_1 through x_0 is unique—even locally.*

In order to verify this, let π_{n-1} be the $(n-1)$-section constructed above. If π'_{n-1} is another $(n-1)$-section through x_0 of a neighborhood $U\subset S_1$ of x_0 on which $p=p(x_0)$, then π'_{n-1} and $\pi_{n-1}(x_j)$ necessarily intersect at a point x_j' in U for j sufficiently large. This is based on the fact that $\pi_{n-1}(x_j)$ and π'_{n-1} are of dimension $n-1$. But by Lemma 2, $x_j'\in\pi_{n-1}(x_j)$ implies that $r^*(x_j')=r(x_j)=1$ and that there is only one $(n-1)$-section (even locally) of S_1 through x_j' on which p is constant. Contradiction. This proves Corollary 2.

As a final consequence of Lemma 2, we prove

THEOREM I. *Let $p=p(x)$ be a gradient mapping with zero Jacobian in D (so that $r(x)<n$ for all x in D). Assume that D is bounded and that p is of class C^1 in D and class C^0 in $\bar{D}$. Then $p(D)$ is contained in $p(D')$.*

Theorems I and II (below) are false if the condition that $p=p(x)$ is a *gradient* mapping is omitted, for we may take $p_1=0$ and $p_2,\cdots,p_n$ arbitrary.

Proof. Assume that the theorem is false. Let A be a component of the set of points x in D such that $p(x)$ is not in $p(D')$. Clearly A is an open set and $p(A')$ is contained in $p(D')$. Let $k = \max r(x)$ for x in A. Then $k < n$ and A is contained in S_k. There exists a point x_0 in A with $r(x_0) = k$; in particular $r(x_0) = r^*(x_0) = k$. According to Lemma 2, there is an $(n-k)$-dimensional section of S_k, hence of A, through x_0 on which $p(x) = p(x_0)$. Consequently $p(x_0)$ is contained in $p(A')$ and hence, in $p(D')$. This contradicts the definition of the set A. Thus Theorem I is proved.

We now present the

Proof of Lemma 2. (a) It will first be shown that in a small neighborhood U of x_0, the x-set $p(x) = p(x_0)$ is a unique $(n-k)$-dimensional plane section of U. Without violating the condition that $p = p(x)$ is a gradient mapping, it can be supposed that the matrix $J_k(x) = (\partial p_\alpha / \partial x_\beta)$, where $\alpha, \beta = 1, \cdots, k$ is non-singular at $x = x_0$. (For otherwise the map $x \to p(x)$ can be replaced by the map $x \to T'p(Tx)$ where T is a suitably chosen constant, non-singular matrix and T' is its transpose.) Hence the mapping $x \to q = (p_1(x), \cdots, p_k(x), x^{k+1}, \cdots, x^n)$ has a nonvanishing Jacobian at x_0, and so q can be introduced as new coördinates in a vicinity U of x_0.

By considering the Jacobian matrix $(\partial p_i / \partial q^j)$, it is seen that the assumption $r(x_0) = r^*(x_0) = k$ implies that $p_{k+1}, \cdots, p_n$ depend only on $(q^1, \cdots, q^k)$ and are independent of $(q^{k+1}, \cdots, q^n) = (x^{k+1}, \cdots, x^n)$. Hence, in U, the relations $p(x) \equiv \text{const.}$ are equivalent to $(q^1, \cdots, q^k) \equiv \text{Const.}$

By (2), $0 = dw = \sum dp_i \wedge dx^i$. Expressing the right side of this equation in q-coordinates, and equating the coefficients of $dq^\alpha \wedge dq^i$ to zero gives

$$\partial x^\alpha / \partial q^j + \partial p_j / \partial q^\alpha = 0 \qquad \text{for } \alpha \leqq k < j.$$

Consequently, we have

$$x^\alpha = \sum_{i>k} a_i^\alpha x^i + b^\alpha \qquad \text{for } \alpha = 1, \cdots, k \tag{4}$$

where $-a_i^\alpha = \partial p_i / \partial q^\alpha$, b^α are functions of $(q^1, \cdots, q^k)$ only. Thus, in U, the hypersurface $p(x) = p(x_0)$ is an $(n-k)$-dimensional plane section of U.

(b) Let $\pi_{n-k} = \pi_{n-k}(x_0)$ be the corresponding $(n-k)$-section of S_k. It will be shown that $p(x)$ is constant on π_{n-k}. Since the change of coordinates $x \to q$ is of class C^1, the functions $a_i^\alpha(q^1, \cdots, q^n)$, $b^\alpha(q^1, \cdots, q^n)$ in (4) are of class C^1. Inserting (4) into $p_\alpha = p_\alpha(x)$ and differentiating with respect to $q_\beta = p_\beta$ gives

$$\delta_{\alpha\beta} = \sum_{\gamma=1}^{k} (\partial p_\alpha / \partial x^\gamma) \sum_{i>k} (x^i \partial a_i^\gamma / \partial q^\beta + \partial b^\gamma / \partial q^\beta) \qquad \text{for } \alpha, \beta = 1, \cdots, k.$$

Hence

$$(5) \quad 1 = \det J_k(x) \cdot \det\Big(\sum_{i>k} (x^i \partial a_i^\alpha / \partial q^\beta + \partial b^\alpha / \partial q^\beta)\Big), \quad \text{where } \alpha, \beta = 1, \cdots, k.$$

We claim that $p(x) = p(x_0)$ and $\det J_k(x) \neq 0$ on π_{n-k}. If not, there exists an arc $x = x(t)$, $0 \leqq t < 1$, on π_{n-k} starting at $x(0) = x_0$ on which either $p(x(t))$ is not constant or $\det J_k(x(t))$ vanishes somewhere. Let $t_0 < 1$ denote the least upper bound of t values for which

$$(6) \qquad p(x(s)) = p(x_0) \text{ and } \det J_k(x(s)) \neq 0$$

holds for $s \leqq t$. It is clear that $p(x(t_0)) = p(x_0)$. Furthermore the coordinate transformation $x \to q$ in part (a), hence (5), is valid in a neighborhood of each point $x(s)$ for $s < t_0$. Along $x = x(s)$, $s < t_0$, the functions $\partial a_i^\alpha / \partial q^\beta$ are independent of s. Hence (5) implies that $\det J_k(x(s))$ is bounded away from zero as $s \to t_0$. Consequently (6) holds at $s = t_0$. Since $x(t_0)$ is a point of π_{n-k}, hence of S_k, it follows that $r^*(x(t_0)) = r(x(t_0)) = k$. Applying the result of (a) at the point $x(t_0)$, it is seen that (6) holds on an s-interval larger than $[0, t_0]$. This is a contradiction, and so $p(x) \equiv p(x_0)$, $r(x) = r^*(x) = k$ on π_{n-k}.

4. Gradient maps with Jacobian not changing sign. We now present our main result.

THEOREM II. *Let $p = p(x)$ be a gradient mapping with Jacobian not changing sign in a bounded domain D, with p of class C^1 in D, C^0 in $\bar{D}$. Then $p'(D)$ is contained in $p(D')$.*

Proof. Assume the theorem to be false. Then there is a point x in D with $p(x)$ in $p'(D)$, but not in $p(D')$. Let A be the connected component, containing x, of the set of points y in D with $p(y)$ not in $p(D')$. Then $p(A') \subset p(D')$. Applying Lemma 1, we see that the Jacobian vanishes identically in A. By Theorem I, it now follows that $p(A)$ is contained in $p(A')$, and hence in $p(D')$. Contradiction!

We remark that under the conditions of the theorem, it is not true that $p(x) \in p(D')$ for every point x where the Jacobian vanishes, as the following example shows: Take $n = 2$ with coordinates (x, y), D the unit circle, and $p = \operatorname{grad}(x^2 y + y^2 x)$. Then $p \neq 0$ except at the origin, while the Jacobian is $-4(x^2 + xy + y^2) \leqq 0$ and vanishes only at the origin.

A simple consequence of Theorem II is

COROLLARY 1. *Let $p = p(x)$ satisfy the conditions of Theorem* II. *Let $F(p)$ be a continuous function defined in the p space satisfying a weak maximum principle on every bounded domain (i.e., the maximum of F on*

the closure of the domain occurs on the boundary). Then the maximum of $F(p(x))$ on $\bar{D}$ occurs on D'.

A particular case is the following:

COROLLARY 2. *Under the conditions of Theorem* II, *each component $p_i(x)$ of $p(x)$ assumes its maximum and minimum on the boundary D'; furthermore, $|p(x)| = (\sum p_k^2(x))^{\frac{1}{2}}$ assumes its maximum on D'.*

Another simple consequence of Theorem II is

COROLLARY 3. *Under the conditions of Theorem* II, *assume that the range of values of p on D' omits an open connected set A in p space. If, for some point x_0 in D, $p(x_0) \in A$, then all the p values in A are taken on by $p(x)$ in D.*

A particular case is

COROLLARY 4. *Under the conditions of Theorem* II, *assume that $|p| \geqq a > 0$ on D', where a is a constant. Then either $|p(x)| \geqq a$ in D or else $p(x)$ assumes in D all values p in the sphere $|p| \leqq a$.*

5. Hypersurfaces with non-simple planar projections. Theorems I and II above may be extended easily to hypersurfaces of dimension n immersed in $(n+1)$-space—without the requirement that the surface be representable in the form $x^{n+1} = z(x^1, \cdots, x^n)$.

We consider differentiably immersed compact pieces of Riemannian manifolds: Let M be a connected open subset of an oriented n-dimensional Riemannian manifold of class C^2 whose closure $\bar{M}$ is compact; denote its boundary by M'. We consider an isometric mapping v: $\bar{M} \rightarrow E^{n+1}$ with the Jacobian matrix everywhere of rank n, so that the mapping is locally one-to-one. This defines an isometric immersion of $\bar{M}$. The mapping is assumed to be of class C^2 in M and of class C^1 in $\bar{M}$.

The letters x, y will be used to denote points on $\bar{M}$ and also to denote local coordinates $x = (x^1, \cdots, x^n)$. We use $v = (v^1, \cdots, v^{n+1})$ to denote coordinates in E^{n+1}.

Let $N(x)$ be the unit normal to $v(\bar{M})$ at the point $v(x)$. Since M is oriented, a fixed choice of $N(x)$ can be made so that $N(x)$ is of class C^1 in M and of class C^0 in $\bar{M}$. Choosing fixed orientations on M and on the unit sphere in E^{n+1}, and denoting by $N(A)$ the image set under the mapping N of a set A in $\bar{M}$ and by $N'(A)$ its boundary (on the surface of the unit sphere), we can extend Theorems I, II as follows:

space, it can be supposed that the x^n axis is perpendicular to the $\pi(x)$. Since $v(x)$ is linear on every $\pi(x)$, it has the form

$$v(x)=\sum_{j=1}^{n-1} a_j(x^n)x^j+b(x^n),$$

where $a_1,\cdots,a_{n-1},b$ are C^2 vectors in v space. From the isometry of the mapping, it is easily verified that $a_1,\cdots,a_n$ are constant vectors and that $a_1,\cdots,a_{n-1}$, $\partial b/\partial x^n$ are orthonormal.

7. Generalization of a theorem of Rado. As above, let E^n be the Euclidean $x=(x^1,\cdots,x^n)$ space. In this section, let E^{n+1} be the Euclidean $(x,z)=(x^1,\cdots,x^n,z)$ space, and call the z axis the vertical axis. The following terminology will be used below: A point set A_1 is said to lie above [or below] a point set A_2 in E^{n+1} if for every pair of points (x,z_1), (x,z_2) of A_1, A_2, respectively, having the same x coordinates, the inequality $z_1\geqq z_2$ [or $z_1\leqq z_2$] holds. By the slope of an n-dimensional hypersurface in E^{n+1} is meant the absolute value of the tangent of the angle between its normal and the z axis.

THEOREM IV. *Let D be a bounded convex domain in the x space E^n. Let $z=z(x)$ be a function of class C^2 on D and of class C^1 on $\bar{D}$. Let the Hessian matrix $(z_{ij}(x))$, where $z_{ij}=\partial^2 z/\partial x^i\partial x^j$, possess both non-negative and non-positive eigenvalues at each point x of D and satisfy*

$$\det(z_{ij}) \text{ does not change sign in } D. \tag{10}$$

(If n is even, these conditions on the Hessian hold, for example, if

$$\det(z_{ij})\leqq 0 \text{ in } D \tag{10'}$$

holds.) Let S be the n-dimensional surface S: $z=z(x)$ in E^{n+1} and S' its boundary. Let K be a number with the property that through every point of S', there pass two n-dimensional planes with slope K such that S' lies above one and below the other. Then $|\operatorname{grad} z(x)|\leqq K$ in D.

If $n=2$, this is implied by a theorem of Rado [8]; cf. von Neumann [6]. In Rado's theorem, the differentiability conditions and (10′) are relaxed to the assumptions that $z(x^1,x^2)$ is continuous on $\bar{D}$ and that, for arbitrary constants a_1, a_2, the function $z(x^1,x^2)-a_1x^1-a_2x^2$ satisfies a weak maximum and minimum principle and the assertion is that $z(x)$ satisfies a Lipschitz condition with K as a Lipschitz constant.

If n is odd, the conditions on the Hessian in Theorem IV cannot be replaced by (10′). This can be seen from the example $z=R^2-|x|^2$ on the sphere D: $|x|<R$.

Theorem IV is false for both odd and even $n(>2)$ if condition (10) is omitted (and, in fact, it is then impossible to find an a priori bound for $|\operatorname{grad} z|$). In order to obtain an example, let $\rho=(x^3)^2+\cdots+(x^n)^2$, so that $|x|^2=(x^1)^2+(x^2)^2+\rho$, and let $k(>\pi)$ be a large constant to be specified below. On the sphere $\bar{D}$: $|x|\leqq 1$, put

$$z(x)=(x^1)^2-(x^2)^2+(1-|x|^2)\sin k\rho.$$

Then

$$\operatorname{grad} z=2(x^1,-x^2,0,\cdots,0)-2x\sin k\rho \\ +2k(1-|x|^2)(0,0,x^3,\cdots,x^n)\cos k\rho.$$

Let $H(x)=(z_{ij}(x))$ be the Hessian matrix of z. The 2 by 2 matrix $(z_{ij}(x))$, where $i,j=1,2$, in the upper left corner of $H(x)$ is a diagonal matrix with diagonal elements $2-2\sin k\rho$, $-2-2\sin k\rho$. Accordingly, $H(x)$ has an eigenvalue $\lambda\geqq 2-2\sin k\rho\geqq 0$ and an eigenvalue $\lambda\leqq -2-2\sin k\rho\leqq 0$. On D': $|x|=1$, $z(x)$ reduces to $z(x)=(x^1)^2-(x^2)^2$, so that there exists a constant K satisfying the assumption of Theorem IV and K can be chosen independent of k. On the other hand, if $x^1=x^2=0$ and $|x|^2=\rho=\pi/k(<1)$, then $|\operatorname{grad} z|=2(1-\pi/k)(\pi k)^{\frac{1}{2}}$. Hence, for such points x, $|\operatorname{grad} z|>K$ if k is sufficiently large. Thus the assertion of Theorem IV is not valid.

In the proof of Theorem IV, we shall need the following simple lemma.

LEMMA 3. Let $z=z(x)$ be a function of class C^2 on a bounded domain D in E^n and of class C^0 on $\bar{D}$. Let the Hessian matrix $(z_{ij}(x))$ have a non-positive [or non-negative] eigenvalue at every point x of D. Then $z(x)$ assumes its minimum [or maximum] value on D'.

Proof of Lemma 3. It is sufficient to verify the non-bracketed part. It can be supposed that $z\geqq 0$ in D'. It will be shown that $z\geqq 0$ on D.

Let $R>0$ be so large that $\bar{D}$ is contained in the sphere $|x|<R$. Put $z_\epsilon=\epsilon(R^2-|x|^2)+z(x)$ for $\epsilon>0$. It suffices to show that $z_\epsilon\geqq 0$ in D for all $\epsilon>0$. For the desired conclusion then follows by letting $\epsilon\to 0$.

It is clear that $z_\epsilon(x)>0$ on D' for all $\epsilon>0$. Suppose that, for some $\epsilon>0$ and some $x_0\in D$, $z_\epsilon(x_0)<0$. Then $z_\epsilon(x)$ has a negative minimum on $\bar{D}$ which is taken at some point, say x_0, of D. Then the matrix $(z_{\epsilon ij}(x_0))$ has only non-negative eigenvalues. But $z_{\epsilon ij}(x_0)=-2\epsilon\delta_{ij}+z_{ij}(x_0)$, so that $(z_{\epsilon ij}(x_0))$ has a negative eigenvalue since $(z_{ij}(x_0))$ has a non-positive one. This contradiction proves Lemma 3.

Proof of Theorem IV. Consider the two n-dimensional planes with slope K through a point of S' such that S' is above one and below the other. An application of Lemma 3 to $z(x)$ plus a linear function shows that, not only S', but S is above one plane and below the other.

It follows that the inequality $|\operatorname{grad} z(x')| \leqq K$ holds at every point x' of D'. Since $z(x)$ is of class C^1 on $\bar{D}$, this inequality certainly holds at a point x' if D' has a tangent (unique supporting) hyperplane at x'. Since such points are dense on D', continuity considerations imply that the inequality holds at all points x' of D'. Theorem IV now follows from Corollary 2 of Theorem II (at the end of Section 4).

Part II ($n = 2$).

In this part we study more closely surfaces ($n = 2$) in 3-space with zero Gauss curvature. We shall make considerable use of Corollary 2 of Lemma 2 in Section 3.

It can be remarked that Lemma 2 and its Corollary 1 imply the following completion of a classical theorem in differential geometry (see also [7]):

Let $S: x^3 = z(x^1, x^2)$ be a surface of class C^2, defined for $(x^1)^2 + (x^2)^2 < 1$. Then the Gauss curvature of S is identically zero if and only if through every point (x^1, x^2, x^3) of S there passes a line segment on S along which the normal vector is constant.

Standard texts give a proof of the "only if" portion of this theorem only under the additional assumption that "*every or no* point of S is a flat (planar) point."

8. On parametrizations by asymptotic lines. The following is an immediate corollary of Lemma 2 and its Corollary 2.

Corollary 3. Let $S: x^3 = z(x^1, x^2)$ in $(x^1)^2 + (x^2)^2 < 1$ be a surface of class C^2 with zero Gauss curvature and with its nonflat points dense on $(x^1)^2 + (x^2)^2 < 1$, so that $r^* \equiv 1$. Then S has a C^0 parametrization of the form

$$x^j = a^j(u)v + b^j(u) \qquad \text{for } j = 1, 2, 3$$

where (u, v) varies over some simply connected plane domain. Here $a = (a^1(u), a^2(u), a^3(u))$ is a continuous unit vector, the vector $b = (b^1(u), b^2(u), b^3(u))$ is of class C^2 and the vector product $[a(u), b_u(u)]$ is not zero and is normal to the surface at the point (u, v).

The unit vector $a(u)$ is, of course, in the direction of the "asymptotic" line segment through the point (u, v) of S. If S has no flat points, then the above parametrization can be chosen of class C^1, but it may not be possible to choose it of class C^2, cf. [4], p. 169. On the other hand, if S contains at least one flat point, hence a line segment of such points, then

it may not be possible to choose such a parametrization of class C^1 (even if z is analytic in x^1 and x^2).

The last statement follows from the example $S: z = (x^2)^4/(2-x^1)^3$. Since $\partial z/\partial x^1 = 3(x^2)^4/(2-x^1)^4$ and $\partial z/\partial x^2 = 4(x^2)^3/(2-x^1)^3$, it follows that $\partial z/\partial x^1 = f(\partial z/\partial x^2)$, where $f(q) = 3(q/4)^{4/3}$. S has the parametrization $x^1 = v, x^2 = (u/4)^{1/3}(2-v)$, $x^3 = (u/4)^{4/3}(2-v)$, which is linear in v, and is such that the normal to S is independent of v. This parametrization is continuous but not of class C^1. An argument similar to that of [4], pp. 169-170, shows that S has no C^1 parametrization of the desired type.

As is seen from the Example in the Introduction (by choosing D_1 to be a triangle), Corollary 3 is false if the assumption $r^* \equiv 1$ is omitted. Corollary 3 has, however, a "local" analogue without this assumption.

Corollary 3′. Let S be a surface of class C^2 with zero Gauss curvature. Then every point of S has a neighborhood which admits a parametrization of the form given in Corollary 3.

Proof. We may always assume that S has the representation $x^3 = z(x)$, $x = (x^1, x^2)$, in a neighborhood of the point in question. Let the point be $(0, 0, 0)$. If $r = 1$ or $r^* = 0$ at the point there is nothing to prove. Thus we only consider the case that $r = 0$ and $r^* = 1$ at the origin. Suppose z is defined in $D: |x| < R$. By Lemma 2 and its Corollaries 1 and 2, we see that through every point x with $r^*(x) = 1$ there is a unique 1-section $l(x)$ of D on which $\operatorname{grad} z$ is constant, these line segments $l(x)$ do not intersect, and $l(x)$ depends continuously on x. We may suppose that $l(0)$ lies on the x^1-axis; then for $|x| \leqq \epsilon$, ϵ small, the lines $l(x)$ are practically parallel to the x^1-axis.

At least one of the half neighborhoods of the origin: $|x| < \epsilon$, $x^2 > 0$ or $x^2 < 0$, say $x^2 > 0$, contains a point y with $r(y) = 1$. Consider the portion $D(y)$ of $|x| \leqq \epsilon$ lying between the line $l(y)$ and the x^1-axis. We shall show that, through every point of $D(y)$, there passes a 1-section of D on which $\operatorname{grad} z = \text{constant}$, that these 1-sections vary continuously, and that no two of them intersect. The set of points in $D(y)$ with $r^* = 1$ is clearly covered by such 1-sections. The remaining points, with $r^* = 0$ form an open set, and each connected component of it is bounded by two arcs on $|x| = \epsilon$ and by two 1-sections on which $r^* = 1$. Clearly the component can be covered by a continuous one parameter family of non-intersecting 1-sections on which $\operatorname{grad} z = \text{constant}$ (since $\operatorname{grad} z$ is constant in the whole component). Thus $D(y)$ may be so covered.

If the half neighbrohood $|x| < \epsilon$, $x^2 < 0$ also contains a point $\bar{y}$ with $r(\bar{y}) = 1$, we repeat this argument and obtain a covering of $D(\bar{y})$ which together with the preceding yield a covering of a whole neighborhood of

$x=0$; the corollary then follows immediately. If the half neighborhood $|x|<\epsilon$, $x^2<0$ contains only points with $r^*=0$, then we may cover it by lines $x^2=$ constant (on which, of course, $\operatorname{grad} z$ is constant). This covering with the preceding yield again a covering of a whole neighborhood of $x=0$.

9. The sets $N(x)=$ constant. We shall consider again surfaces $x^3=z(x)=z(x^1,x^2)$ with simple projection on a domain D of the $x=(x^1,x^2)$ plane, and shall make some attempt to characterize the sets of D on which N, the normal—or what is the same, $p=\operatorname{grad} z$—can be constant. Thus in the following $p(x)$ is a gradient mapping, with zero Jacobian, defined in a domain D (not necessarily bounded) in the plane; p is of class C^1 in D and of class C^0 in $\bar{D}$.

Definition. For any point x_0 of D, let $C(x_0)$ be the arcwise connected component, containing x_0, of the set of points x for which $p(x)=p(x_0)$.

The following assertions concerning $C(x_0)$ will be proved:

THEOREM A. (a) *If $x\in D$ is a boundary point of $C(x_0)$, then there is a 1-section of D through x belonging to the boundary of $C(x_0)$. Thus, the boundary of $C(x_0)$ consists of 1-sections of D and a subset of the boundary D' of D.* (b) *If D is simply connected and contains a closed line segment $[x_1 x_2]$, where the endpoints are points of $C(x_0)$, then $C(x_0)$ contains the line segment $[x_1 x_2]$. In particular, if D is convex, so is $C(x_0)$.*

It is easy to see that (b) is false if D is not simply connected.

Also, in space, (b) is false. In fact let $n=3$, write (x,y,z) for x, and let $p=\operatorname{grad}(x+z^2(1-y^2)^2)=(1,-4yz^2(1-y^2),2z(1-y^2)^2)$, so that the Jacobian vanishes identically. The set $p=(1,0,0)$ consists of the three planes $z=0$, and $y=\pm 1$. Since this set is arcwise connected, it is $C(0,0,0)$, but it is not convex.

Proof of Theorem A. Since a point x in D which is in $C(x_0)$ belongs also to the boundary of $C(x_0)$ if and only if $r^*(x)=1$, part (a) of the theorem follows from Lemma 2 and its Corollary 1. In order to prove part (b) suppose that the segment $[x_1 x_2]$ contains a point x not in $C(x_0)$. It may be supposed that $p(x)\neq p(x_0)$, $r^*(x)=1$. By Lemma 2, p is constant on a 1-section S of D through x, which necessarily has x_1, x_2 on opposite sides. In case D is convex, this contradicts the connectedness of $C(x_0)$ and proves (b) in this case. In general, the connectedness of $C(x_0)$ implies that not both endpoints of S are at infinity.

Let $\mathscr{C}$ be an arc in $C(x_0)$ joining x_1 and x_2. It can be supposed that $\mathscr{C}$ does not meet the open segment $[x_1 x_2]$, for otherwise x_1 can be replaced by

the last intersection x_1', going from x_1 to x_2, of $\mathscr{C}$ and the segment $[x_1 x]$, and x_2 by the first intersection after x_1' of $\mathscr{C}$ and the segment $[x x_2]$. By a similar argument it can be supposed that $\mathscr{C}$ has no self intersections. Thus $\mathscr{C}$ together with $[x_1 x_2]$ forms a simple closed curve in D, which by the Jordan curve theorem, has one endpoint of S inside it and the other outside. Since the endpoints of S are boundary points of D this contradicts the assumption that D is simply connected, and proves (b).

Remark. In case D is a bounded convex domain, then a subset D_1 is a possible region $C(x_0)$ if and only if it is of the form in the Example of the Introduction.

We now prove the existence of rays on which p is constant. First a *definition*: Let $x_0 \in D$. By a ray from x_0 in D we mean the connected portion, containing x_0, of the intersection of D with a half infinite straight line having x_0 as endpoint.

THEOREM B. *If $x_0 \in D$, then there exist at least two rays emanating from x_0 on which p is constant. If D has the property that it contains no infinite (in both directions) straight line and if $r^*(x_0) = 0$, then there are at least three such rays from x_0.*

Proof. In view of Lemma 2 and its Corollary 1, it can be supposed that $r^*(x_0) = 0$, so that x_0 is an interior point of $C(x_0)$. Furthermore, we may suppose that D is star shaped about x_0, and so, simply connected, otherwise, we restrict ourselves to the star-shaped domain made up of all rays from x_0 in D.

Consider a ray from x_0 on which p is not constant. (If none such exists, we have nothing more to prove.) Moving along the ray from x_0 we come to a first point x_1 of D belonging to the boundary of $C(x_0)$, so that $r^*(x_1) = 1$. Let $\pi(x_1)$ be the 1-section through x_1 of Theorem A(a) on which p is constant. It follows from Theorem A(b) that the straight segment joining x_0 to any point of $\pi(x_1)$ belongs to $C(x_0)$, so that p is constant on it. But then it follows that p is constant on the straight segments joining x_0 to the endpoints of $\pi(x_1)$ (which may be at infinity). These segments are rays of D from x_0, so that we have shown the existence of two rays having the required property.

Suppose now that D contains no infinite straight line. Then the triangle made up by the straight segments from x_0 to points of $\pi(x_1)$ above, on which p is constant, has an angle at the vertex x_0 smaller than π. Let us now consider a ray from x_0 in D which does not belong to the triangle and on which p is not constant. Repeating the argument above we obtain a 1-section

$\pi(x_1')$ such that p is constant on the straight segment joining x_0 to any point of it. But the sections $\pi(x_1)$, $\pi(x_1')$ can have at most one endpoint in common. Thus we have three distinct rays from x_0 on which p is constant.

Remark 1. That there need not exist more than three such rays can be seen from the Example in the Introduction, where for D_1 we take a triangle with vertices on the boundary of D. Then D_1 serves as a set $C(x_0)$ for any point x_0 inside it, and from any such point, the only rays on which p is constant are those to the vertices of D_1.

Remark 2. The proof of Theorem B shows for *any* D that if, from x_0 in D, there are two non-collinear rays on which p is constant, then there is a third.

THE JOHNS HOPKINS UNIVERSITY.
NEW YORK UNIVERSITY AND UNIVERSITY OF ROME.

REFERENCES.

[1] T. Bonnesen and W. Fenchel, *Theorie der konvexen Körper*, New York (1948), p. 76.

[2] S. S. Chern and R. K. Lashof, "The total curvature of immersed manifolds," *American Journal of Mathematics*, vol. 79 (1957), pp. 308-318.

[3] A. Douglis, "An extremum problem for solutions of a class of elliptic systems of differential equations with continuous coefficients," *Proceedings of the International Congress of Mathematics*, vol. 1 (1950), pp. 431-432, Cambridge (Mass.).

[4] P. Hartman and A. Wintner, "On the asymptotic curves of a surface," *American Journal of Mathematics*, vol. 73 (1951), pp. 149-172.

[5] K. Knopp and R. Schmidt, "Funktionaldeterminanten und Abhängigkeit von Funktionen," *Mathematische Zeitschrift*, vol. 25 (1926), pp. 373-381.

[6] J. von Neumann, "Ueber einen Hilfssatz der Variationsrechnung," *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität*, vol. 8 (1931), pp. 27-31.

[7] A. Pogorelov, "On continuous mappings of bounded variation" and "An extension of Gauss' theorem on the spherical representation of surfaces of bounded exterior curvature," *Doklady Akademii Nauk*, vol. 111 (1956), pp. 757-759 and 945-947.

[8] T. Rado, "Geometrische Betrachtungen über zweidimensional reguläre Variationsprobleme," *Acta Litterarum ac Scientiarum (Szeged)*, vol. 2 (1924), pp. 228-253.

[9] A. Sard, "The measure of the critical values of differentiable maps," *Bulletin of the American Mathematical Society*, vol. 48 (1942), pp. 883-890.

[10] A. Wintner, "On Riemann metrics of constant curvature," *American Journal of Mathematics*, vol. 73 (1951), pp. 569-575.

[11] G. S. Young, "Generalizations of the Liouville theorem to higher dimensions," *Notices of the American Mathematical Society*, vol. 5 (1958), pp. 208, Abstract No. 544-10.

COLLINEATION GROUPS OF NON-DESARGUESIAN PLANES, I.*

The Hall Veblen-Wedderburn systems

By D. R. Hughes.[1]

1. Introduction. In the modern study of projective planes, a problem of considerable interest is that of determining the collineation groups of the known non-Desarguesian planes. For the group reveals much about the structure of the plane, and interesting problems of group theory can be involved. Perhaps the most thorough investigation of this sort to date is due to Zappa ([9]); he determined at least part (and possibly all) of the collineation group of a typical "Hughes plane," showing among other things that the group is necessarily not solvable. Essentially, this was because the collineation group contains a subgroup isomorphic to a three dimensional projective group. In this paper we shall show that the collineation group of a Hall Veblen-Wedderburn plane contains the two dimensional general linear group over an appropriate field; this group is non-solvable with certain exceptions. The only exceptional case that interests us (when the field under consideration is $GF(3)$) is shown to give rise to a non-solvable group for other reasons. Also, the whole collineation group of a finite Hall Veblen-Wedderburn plane is determined.

In Section 2 the Hall Veblen-Wedderburn systems are defined. Sections 3 and 4 are concerned, respectively, with existence and uniqueness theorems on collineations of the planes. In Section 5 we find conditions that non-isomorphic systems shall coordinatize the same plane; in particular, it is shown that two finite Hall Veblen-Wedderburn planes of the same order are isomorphic. Section 6 is concerned with the exceptional plane of order 9, which is the same as the problem of the field $GF(3)$ mentioned above.

Since this research was carried out, it has been shown by Albert that the planes coordinatized by "twisted fields" have solvable collineation groups, and still more recently the author has shown that all the other known finite non-associative division rings give planes with solvable collineation groups. It is not clear what conclusions, if any, should be drawn from these facts.

The author would like to thank Marshall Hall for several helpful con-

* Received February 6, 1959.

[1] Supported in part by the Office of Ordnance Research.

versations about this paper; in particular, he pointed out the truth of Lemma 5.1 and Theorem 6.1, thus filling what would have otherwise been gaps in the treatment.

2. The Hall Veblen-Wedderburn systems. For a background on the notion of the most general coordinatizing system for projective planes, see [2, 3, 7] and in particular [3] for the scheme used here. We shall only be interested in a special type of coordinate system and we restrict attention to that system.

Suppose R is a set containing at least the two distinct elements 0 (zero) and 1 (one), and possessing two binary operations, addition and multiplication. We let R^* denote the set of non-zero elements of R. If the following are satisfied, then R is called a *left Veblen-Wedderburn system* (left V-W system, or merely V-W system, for short):

(a) $(R, +)$ is a group with "identity" zero;

(b) $(R^*, \cdot)$ is a loop with identity 1;

(c) $a(b+c) = ab + ac$, for all a, b, c in R;

(d) if a, b, c in R, $a \neq b$, then there is a unique x in R such that $ax = bx + c$.

It has been shown that then $(R, +)$ is necessarily abelian, and if R is finite, $(R +)$ is even elementary abelian, so that the order of R, (i.e., number of elements) is a prime power. Furthermore, if R is finite, then (d) is redundant. (See [7] for proofs.) If we wish to emphasize the operations of R, we write $(R, +, \cdot)$.

If R is a V-W system, a projective plane π is constructed from R as follows: the points of π are the symbols (x, y), (x), (∞) for all x, y in R, and where "∞" is a symbol not in R; the lines of π are the symbols $[m, k]$, $[\infty, (k, 0)]$, L_∞, for all m, k in R. The incidence rules of π are: (x, y) is on $[m, k]$ if $mx + y = k$, and (x, y) is on $[\infty, (k, 0)]$ if $x = k$; (x) is on $[m, k]$ if $x = m$, and (x) is on L_∞; (∞) is on L_∞ and on $[\infty, (k, 0)]$. (Again, see [2, 3, 7] for more details.) A *collineation* of π (indeed, of any projective plane) is a one-to-one mapping of points onto points, lines onto lines, which preserves incidence.

If π is a projective plane coordinatized by a V-W system (e.g., as above), then it is known ([2, 7]) that every coordinate system for π with the same choice of L_∞ (the line at infinity) is also a V-W system (not neces-

sarily isomorphic), and if R is not an alternative division ring, then no other choice of the line at infinity will lead to a coordinate ring which is a V-W system. Hence in particular, if R is a V-W system but not an alternative division ring, no collineation of π can move the line L_∞. (We recall that finite alternative division rings are fields.)

Now we proceed to the construction of a class of V-W systems. Let $K \neq GF(2)$ be any field over which there exist irreducible quadratics, and let $f(z) = z^2 - pz - q$ such an irreducible quadratic over K.[2] Define R to be the set of all elements $\lambda a + b$, where a, b are in K (and λ is a new symbol), with an addition in R given by:

$$(1) \qquad (\lambda a + b) + (\lambda c + d) = \lambda(a + c) + (b + d).$$

Define multiplication in R by:

$$(2) \quad (\lambda \cdot 0 + b)(\lambda c + d) = \lambda(bc) + (bd),$$

$$(3) \quad \text{if } a \neq 0, \text{ then } (\lambda a + b)(\lambda c + d) = \lambda(ad - bc + pc) + bd - a^{-1}c(b^2 - pb - q).$$

Then R is a left V-W system, never satisfies the right distributive law, and never satisfies the associative law for multiplication except in the single instance that $K = GF(3)$ and $p = 0$, $q = -1$. (Proofs are in [2, 7].) Such a system will be called a *Hall V-W system*, and the projective plane coordinatized by it a Hall V-W plane. Since the set of elements of the form $\lambda \cdot 0 + b$ forms a subfield isomorphic to K, we will identify this subset with K.

It is not at all hard to prove, using (2), (3) above, that the following rules hold in R:

(4) if a is in R, then $ax = xa$ for all x in R if and only if a is in K;

(5) if a is in R, then $(xy)a = x(ya)$ for all x, y in R if and only if a is in K, or $K = GF(3)$, $p = 0$, $q = -1$, in which case a can be any element of R;

(6) if x is in R, but not in K, then $x^2 = px + q$.

Indeed, Hall's original definition ([2]) of these systems was made by means of (1), (4), (5), (6), whence one can show (2), (3) as consequences. In view of (4) and (5), we call K the *center* of R.

The automorphism group of R has been determined in [4]; we will give

[2] In case $K = GF(2)$, the resulting system is $GF(4)$; for certain purposes, $GF(4)$ does indeed behave like a Hall V-W system, but the exceptions are numerous enough to warrant excluding it from consideration here.

it after giving a larger group of "autotopisms" which turns out to have considerable importance. Let a, b, c, d be in K, with $ad - bc \neq 0$, and define $S = S(a, b, c, d)$ to be the following mapping of R (clearly one-to-one and onto):

$$(\lambda x + y)S = \lambda(ax + by) + (cx + dy).$$

Then (see [6]), S satisfies:

(7) $(x + y)S = xS + yS$, for all x, y in R;

(8) $(xy)S = (xs)S(yS)$, for all x, y in R, where s is the element defined by $sS = 1$.

Furthermore:

(9) if x, y, u, v are in R, $y \neq 0$, $v \neq 0$, x not in Ky, u not in Kv, then there is a unique mapping $S = S(a, b, c, d)$ such that $xS = u$, $yS = v$.

If $\mathfrak{B}$ is the set of all mappings $S(b, 0, a, 1)$, with $b \neq 0$, then the automorphism group of R is the direct product of the group $\mathfrak{B}$ and the group of automorphisms of K which fix the elements p and q. The group $\mathfrak{B}$ is transitive on the set of elements of R which are not in K, and thus, if it is convenient, we can choose λ, say, as a "typical" element of R which is not in K.

3. Existence of collineations. Now let R be the Hall V-W system constructed over the field K using the irreducible quadratic $f(z) = z^2 - pz - q$, and let π be the projective plane coordinatized by R. We shall proceed to exhibit various collineations of π.

(1) The translation group $\mathfrak{T}$; this group is possessed by all V-W planes. For each pair a, b in R, define $\tau = \tau(a, b)$ by:

$$\begin{array}{ll} \tau\colon (x, y) \to (x + a, y + b) & [m, k] \to [m, k + ma + b] \\ \quad (x) \to (x) & [\infty, (k, 0)] \to [\infty, (k + a, 0)] \\ \quad (\infty) \to (\infty) & L_\infty \to L_\infty. \end{array}$$

(2) The automorphism group $\mathfrak{A}$. For each automorphism α of K which fixes p and q, define α on R by $(\lambda x + y)\alpha = \lambda(x\alpha) + (y\alpha)$, and then define α on π by:

$$\begin{array}{ll} \alpha\colon (x, y) \to (x\alpha, y\alpha) & [m, k] \to [m\alpha, k\alpha] \\ \quad (x) \to (x\alpha) & [\infty, (k, 0)] \to [\infty, (k\alpha, 0)] \\ \quad (\infty) \to (\infty) & L_\infty \to L_\infty. \end{array}$$

(3) The multiplication group $\mathfrak{M}$. If a is in K^*, let $\mu = \mu(a)$ be defined by:

$$\begin{array}{ll} \mu\colon (x,y) \to (xa, ya) & [m,k] \to [m, ka] \\ \quad (x) \to (x) & [\infty, (k,0)] \to [\infty, (ka,0)] \\ \quad (\infty) \to (\infty) & L_\infty \to L_\infty. \end{array}$$

(4) The autotopism group $\mathfrak{S}$. For each mapping S, as defined in Section 2, define $\sigma = \sigma(S)$ as follows:

$$\begin{array}{ll} \sigma\colon (x,y) \to (xS, yS) & [m,k] \to [(ms)S, kS] \\ \quad (x) \to ((xs)S) & [\infty, (k,0)] \to [\infty, (kS,0)] \\ \quad (\infty) \to (\infty) & L_\infty \to L_\infty. \end{array}$$

Here, as in Section 2, s is the element defined by $sS = 1$. Note that $\mathfrak{M} \subseteq \mathfrak{S}$, since if $S = S(a,0,0,a)$, then $\sigma(S) = \mu(a)$.

(5) The linear group $\mathfrak{L}$. For each choice of a, b in K, not both zero, define $\zeta = \zeta(a,b)$ by:

$$\begin{array}{l} \zeta\colon (x,y) \to ((pa+b)x + ay, qax + by) \\ \quad (x) \to (x), \text{ if } x \text{ is not in } K \\ \quad (x) \to (-(xb-qa)(xa-pa-b)^{-1}), \text{ if } x \text{ is in } K, \text{ but } xa \neq pa+b. \\ \quad (p+ba^{-1}) \to (\infty), \text{ if } a \neq 0 \\ \quad (\infty) \to (-ba^{-1}), \text{ if } a \neq 0 \\ \quad (\infty) \to (\infty), \text{ if } a = 0 \\ \quad [m,k] \to [m, mka + bk], \text{ if } m \text{ is not in } K \\ \quad [m,k] \to [-(mb-qa)(ma-pa-b)^{-1}, \\ \qquad\qquad\qquad -k(b^2+pab-qa^2)(ma-pa-b)^{-1}], \\ \qquad\qquad\qquad \text{if } m \text{ is in } K, \text{ but } ma \neq pa+b \\ \quad [p+ba^{-1}, k] \to [\infty, (ka,0)], \text{ if } a \neq 0 \\ \quad [\infty, (k,0)] \to [-ba^{-1}, -ka^{-1}(b^2+pab-qa^2)], \text{ if } a \neq 0 \\ \quad [\infty, (k,0)] \to [\infty, (kb,0)], \text{ if } a = 0 \\ \quad L_\infty \to L_\infty. \end{array}$$

Note also that $\mathfrak{M} \subseteq \mathfrak{L}$, since $\zeta(0,a) = \mu(a)$.

(6) The involution δ defined by:

$$\begin{array}{ll} \delta\colon (x,y) \to (-x, px+y) & [m,k] \to [-m+p, k] \\ \quad (x) \to (-x+p) & [\infty, (k,0)] \to [\infty, (-k,0)] \\ \quad (\infty) \to (\infty) & L_\infty \to L_\infty. \end{array}$$

Excepting the cases of the linear group $\mathfrak{L}$ and the involution δ, it is obvious that the above mappings are collineations. We will sketch the proofs for these cases before proceeding to a discussion of the various groups.

Consider $\zeta(a,b)$ in $\mathfrak{L}$. Suppose (x,y) is on $[m,k]$, whence $mx+y=k$. Then if m is not in K, we must show that

$$m[(pa+b)x+ay]+qax+by=m(mx+y)a+b(mx+y).$$

Straightforward simplification reduces the above equation to:

$$mx(pa+b)+mya+qax+by=[m(mx)+my]a+mxb+yb,$$

which reduces to

$$mxp+qx=m(mx)$$

if $a\neq 0$, and if $a=0$ we are done. Now we can assume that $m=\lambda$ and $x=\lambda u+v$, where u, v are in K. Then we have:

$$\lambda(\lambda u+v)p+(\lambda u+v)q=\lambda[\lambda(\lambda u+v)],$$

which is easy to verify, using the fact that $\lambda^2=\lambda p+q$.

On the other hand, if m is in K, $ma\neq pa+b$, then the equation to be checked is:

$$-(mb-qa)[(pa+b)x+ay](ma-pa-b)^{-1}+qax+by$$
$$=-(mx+y)(b^2+pab-qa^2)(ma-pa-b)^{-1}.$$

Since only x and y might not be in K, this equation is easily simplified and verified.

The remaining possiblities are either trivial or similarly straightforward, and so $\mathfrak{L}$ is a collineation group. Note that the one-to-one-ness of $\zeta(a,b)$ is assured by the fact that $b^2+pab-qa^2$ is zero only if $a=b=0$; for if $a\neq 0$, say, then $b^2+pab-a^2=a^2(c^2-pc-q)=a^2f(c)\neq 0$, where $c=-ba^{-1}$. The verification that δ is a collineation is similar, while the assertion than δ is an involution (i.e., $\delta^2=$ identity) is immediate.

We remark that the subset of π consisting of L_∞, (∞), and all points and lines all of whose coordinates are in K is a subplane of π; we will call this subplane π'. Clearly π' is Desarguesian, with K as its coordinate field (see [7]). We shall let π'_∞ denote the set of points of π' which are on L_∞, and for convenience, $L_\infty-\pi'_\infty$ will denote the set consisting of the remaining points on L_∞. By the *finite points* of π (or π') we will mean the set of points of π (or π') which are not on L_∞. Finally, $\mathfrak{G}$ will denote the group of all collineations of π.

THEOREM 3.1. *The groups of collineations given above have the following properties:*

(a) $\mathfrak{T}$ *is transitive on the finite points of* π *and is normal in* $\mathfrak{G}$.

(b) $\mathfrak{S}$ *fixes every point of* π'_∞ *and is transitive on* $L_\infty - \pi'_\infty$.

(c) $\mathfrak{L}$ *fixes every point of* $L_\infty - \pi'_\infty$ *and is transitive on* π'_∞.

(d) $\mathfrak{M} = \mathfrak{S} \cap \mathfrak{L}$.

(e) *If* $\mathfrak{B} = \{\mathfrak{L}, \delta\} =$ *group generated by* $\mathfrak{L}$ *and* δ, *then* $[\mathfrak{B} : \mathfrak{L}] \leqq 2$.[3]

(f) $\mathfrak{S}$ *is isomorphic to the group of all non-singular two-rowed square matrices over* K, *and hence is non-solvable if* K *has more than three elements.*

(g) $\mathfrak{L}$ *is isomorphic to the multiplicative group of the quadratic extension field* $K[w]$, *where* $w^2 = pw + q$.

Proof. (a) is well-known, see for instance [7]. The proof of (b) will be found in [6]. (c) is immediate from the definition of $\mathfrak{L}$, while (d) and (e) are straightforward. Noting the fact that the mapping S acts on the two-dimensional vector space R (over K) exactly as a linear transformation, (f) is clear. Finally, (g) is evident when we set up the correspondences:

$$\zeta(a, b) \leftrightarrow \begin{bmatrix} pa + b & a \\ qa & b \end{bmatrix} \leftrightarrow aw + b \text{ in } K[w].$$

We shall see later that when $K \neq GF(3)$, then $\mathfrak{S}$ and $\mathfrak{L}$ are both normal in $\mathfrak{G}$; it can be demonstrated that under any circumstances each normalizes the other. Indeed, it will be one of our aims to show that we have given essentially all of $\mathfrak{G}$, except in the case that $K = GF(3)$ or K is infinite. Specifically, we shall show that $\mathfrak{G}/\mathfrak{T} \cong \mathfrak{B}\mathfrak{S}\mathfrak{A}$. In order to achieve this, we must show that every collineation of π maps π'_∞ into itself, and so although π' is not an invariant subplane, its intersection with L_∞ is invariant.

4. Uniqueness of collineations. We shall examine here the possibility that other collineations than those generated by the groups of Section 3 can exist. From [6], π possesses a collineation group fixing π'_∞ pointwise, also fixing $(0, 0)$, and transitive on the points $(x, 0)$, $x \neq 0$, of the x-axis (in fact, $\mathfrak{S}$ is the necessary group); certainly $\mathfrak{T}$ is transitive on the finite points of π. So if two different coordinatizations of π exist, using the same points (∞), (0), (1), such that one of the two (at least) is a Hall V-W system, then we

---

[3] $[\mathfrak{B} : \mathfrak{L}] = 2$ excepting possibly in an infinite field of characteristic two, where δ will be the identity if $p = 0$.

can assume that both use the same points $(0,0)$ and $(1,0)$ (and hence the same points $(1,1)$ and $(0,1)$ also). Thus if the set R of symbols is assumed to be the same for both systems, it is easy to show (see [2, 7] for instance) that R has a permutation ϕ, where $0\phi=0$, $1\phi=1$, such that the two systems $(R,+,\cdot)$ and $(R,\oplus,*)$ are related by:

$$(x \oplus y)\phi = x\phi + y\phi, \qquad (x * y)\phi = (x\phi)(y\phi).$$

That is, the two systems are isomorphic.

If $(R,+,\cdot)$ is a Hall V-W system over the field K ($=$ its center), then $(R,\oplus,*)$ is a Hall V-W system over the field $K'=K\phi^{-1}$. If K_1 is the prime field of K, then $K_1=K_1\phi$, so that the set of symbols in K_1 make up the prime field of K' also. (We shall see that for our purposes we can even take $K'=K$.)

Suppose π is finite, with order n; then L_∞ contains $n+1$ points, while π'_∞ contains $n^{\frac{1}{2}}+1$ points. Since $n^{\frac{1}{2}}+1$ never divides $n+1$, it follows that if a collineation of π moves π'_∞, then there are some pairs of images of π'_∞ which are not equal but have a non-empty intersection. So if a collineation moves π'_∞, there is a collineation moving π'_∞ but keeping the point (∞) fixed (since $\mathfrak{G}$ is transitive on π'_∞). This argument breaks down in the infinite case, and so we restrict attention to finite Hall V-W systems excepting insofar as some of the results have restricted validity for infinite systems. Thus we now consider the situation that (∞) is fixed; our conclusions will be valid for collineations of infinite planes which fix π'_∞.

So we suppose that a collineation of π moves (0) to (r), (1) to (s), and fixes (∞) and $(0,0)$. We will investigate a coordinate system for π (using primes for the new coordinates) which has $(\infty)'=(\infty)$, $(0)'=(r)$, $(1)'=(s)$, $(0,0)'=(0,0)$. From the remarks above, we can complete the coordinatization in any convenient fashion, and must arrive at a Hall V-W system isomorphic to $(R,+,\cdot)$. Let $(x,0)'=(x,-rx)$. Then since $(1)'$, $(0,y)'$, and $(y,0)'$ are collinear, it follows that $(0,y)'=(0,sy-ry)$. Since $(x,y)'$ is collinear first with $(\infty)'$ and $(x,0)'$ and second with $(0)'$ and $(0,y)'$, one easily shows that $(x,y)'=(x,sy-ry-rx)$. Finally, $(m)'$ is collinear with $(1,0)'$ and $(0,m)'$, so $(m)'=(sm-rm+r)$.

It is easy to show that in the new system, which we will call $(R,\oplus,*)$, the addition is unchanged: $x\oplus y=x+y$. The multiplication is as follows: if $m*x=k$, then $(m)'=(sm-rm+r)$ and $(x,0)'=(x,-rx)$ are collinear with $(0,k)'=(0,sk-rk)$. So:

$$(1) \qquad (sm-rm+r)x-rx=sk-rk.$$

LEMMA 4.1. *The set of elements of K is precisely the center of the system* $(R, \oplus, *)$.

Proof. It is easy to show that the only elements of a Hall V-W system which distribute on *both* sides are the elements of its center. Now let x be in K, in (1). Then we have $smx - rmx = sk - rk$, or $s(mx - k) = r(mx - k)$, whence $m * x = k = mx$, since $s \neq r$. So $(u \oplus v) * x = (u \oplus v)x = x(u \oplus v) = x(u + v) = xu + xv = ux + vx = u * x \oplus v * x$, for any u, v in R. Hence K must be in the center of $(R, \oplus, *)$. But $(R, \oplus)$ is the same two-dimensional vector space over K as it is over its own center, since $+$ and $\oplus$ are the same operation. Thus it follows that K is precisely the center of $(R, \oplus, *)$.

THEOREM 4.1. *If K is finite and $K \neq GF(3)$, then no collineation of π moves a point of π'_∞ outside of π'_∞.*

Proof. It suffices to show that r and s must be in K. We let m be in K, whence $k = m * x = mx$, from Lemma 4.1.

Case 1. Suppose r is in K, but s not in K; we take $s = \lambda$, without loss of generality. If $x = \lambda a + b$, and m is in K, then (1) becomes:

$$(\lambda m + r - rm)(\lambda a + b) - r(\lambda a + b) = \lambda(\lambda ma + mb) - r(\lambda ma + mb). \tag{2}$$

If $m \neq 0$, this simplifies to:

$$\begin{aligned} \lambda[a(p + rm - 2r) + bm] - m^{-1}a[(r - m)^2 - p(r - rm) - q] - brm \\ = \lambda[a(pm - rm) + bm] + qam - brm. \end{aligned} \tag{3}$$

Since a and b are arbitrary, (3) leads to:

$$\lambda[p - pm + 2rm - 2r] - m^{-1}[(r - rm)^2 - p(r - rm) - q] - qm = 0. \tag{4}$$

Equating coefficients to zero, we have:

$$p(1 - m) - 2r(1 - m) = 0. \tag{5}$$

$$qm^2 + (r - m)^2 - p(r - m) - q = 0. \tag{6}$$

If $m \neq 1$, then (5) yields $p = 2r$; substituting this in (6), we have:

$$m^2(q + r^2) = q + r^2. \tag{7}$$

Thus $m^2 = 1$ or $q = -r^2$. But if $q = -r^2$, then $f(z) = z^2 - pz - q = (z - r)^2$, which is impossible, as $f(z)$ is irreducible, and so $m^2 = 1$. So the only non-zero values in K that m can take are $+1$ and -1; hence $K = GF(3)$.

Case 2. Suppose s is in K and r is not in K; we assume $r=\lambda$. As above, let $x=\lambda a+b$. Then if m is in K, but $m\neq 1$, equation (1) becomes:

$$(8)\qquad \lambda(pm-2sm)-q+qm-(1-m)^{-1}(s^2m^2-psm-q)=0.$$

From $pm-2sm=0$, we deduce $p=2s$, by letting m be non-zero. From the second coefficient in (8), this yields:

$$(9)\qquad m(s^2+q)-2(s^2+q)=0.$$

As before, $s^2+q=0$ implies $f(z)=(z-s)^2$, which is a contradiction, so we must have $m=2$. So if m is in K, it must have one of the values 0, 1, 2, and thus again $K=GF(3)$.

Case 3. Suppose neither s nor r are in K, and $r=\lambda$, $s=\lambda a+b$, where $a\neq 0,1$. As before, let m be in K, and $x=\lambda u+v$. First let $m=(1-a)^{-1}$, whence (1) becomes:

$$(10)\qquad \lambda(ap+2b-p)+aq+a^{-1}(b^2-pb-q)=0.$$

Equating coefficients to zero, we have $p=2b(1-a)^{-1}$ from the λ term, and then from the second term:

$$(11)\qquad q(1-a)(a^2-1)=b^2(a+1).$$

If $a=-1$, then (11) is valid. If $a\neq -1$, then (11) yields $q=-b^2(1-a)^{-2}$, and then $f(z)=[z-b(1-a)^{-1}]^2$, which is impossible. So $a=-1$, and also $p=b$.

Now we assume that $m\neq(1-a)^{-1}=2^{-1}$, $p=b$ in (1), obtaining:

$$(12)\qquad (1-2m)^{-1}(p^2m^2-p^2m-q)+q=2qm,$$

and on simplification, this is:

$$(13)\qquad m^2(p^2+4q)-m(p^2+4q)=0.$$

If K does not have characteristic two, then p^2+4q is the discriminant of $f(z)$, hence is not zero, so (13) implies that $m=0$ or $m=1$; thus once again we are led to $K=GF(3)$. If $2=0$ in K, then $a=-1=1$ and this violates the assumption of Case 3.

Case 4. Suppose $r=\lambda$, $s=\lambda+b$, where $b\neq 0$ of necessity. As before, we take m in K, $x=\lambda u+v$, and equation (1) becomes:

$$(14)\qquad b^2(m^2-m)=0.$$

Since $b\neq 0$, this implies $m=0$ or $m=1$, so $K=GF(2)$, which is impossible.

Thus if $K \neq GF(3)$, we have shown that r and s must be in K, so we are done with the proof of the theorem.

THEOREM 4.2. *If K is finite, $K \neq GF(3)$, then $\mathfrak{G} = \mathfrak{B}\mathfrak{S}\mathfrak{A}\mathfrak{T}$, and both $\mathfrak{S}$ and $\mathfrak{L}$ are normal in $\mathfrak{G}/\mathfrak{T}$.*

Proof. Suppose γ is a collineation of π which fixes (∞), $(0,0)$, and maps π'_∞ into itself. We can represent γ as below, where T, U, V, W, Z are appropriate mappings of R, or $R \times R$, onto R.

$$\begin{aligned}\gamma\colon (x,y) &\to ((x,y)T, (x,y)U)\\ (x) &\to (xV)\\ [m,k] &\to [mV, (m,k)W]\\ [\infty, (k,0)] &\to [\infty, (kZ,0)].\end{aligned}$$

If $x = k$, then $((x,y)T, (x,y)U)$ is on $[\infty, (kZ,0)]$, so $(x,y)T = xZ$. Hence we redefine T so that $xT = xZ = (x,y)T$. If (x,y) is on $[m,k]$, then $mx + y = k$ and:

$$mV \cdot xT + (x,y)U = (m, mx+y)W. \tag{15}$$

If $x = 0$ in (15), then $(m,y)W = (0,y)U$, since $0T = 0$. So we redefine W so that $kW = (m,k)W$. Then (15) is:

$$mV \cdot xT + (x,y)U = (mx+y)W. \tag{16}$$

Letting $m = 0$ and noting that $0V = r$, where r is in K, (16) yields $(x,y)U = yW - r(xT)$, so (16) becomes:

$$mV \cdot xT + yW - r \cdot xT = (mx+y)W. \tag{17}$$

Now let $m = 1$, $y = 0$ in (17), and note that $1V = s$, where s is in K; we have then $xW = s \cdot xT - r \cdot xT = (s-r)xT$. Then (17) is:

$$mV \cdot xT - r \cdot xT + (s-r)yT = (s-r)[(mx+y)T]. \tag{18}$$

If $m = 1$ in (18), then we have $(s-r)xT + (s-r)yT = (s-r)[(x+y)T]$, so $(x+y)T = xT + yT$, since $s \neq r$. So we have:

$$mV \cdot xT - r \cdot xT = (s-r)[(mx)T]. \tag{19}$$

Noting that T is one-to-one and onto, let t in R satisfy $tT = 1$. Letting $x = t$ in (19), we find:

$$mV = (s-r)[(mt)T] + r, \tag{20}$$

$$[(s-r)\cdot(mt)T + r] \cdot xT - r \cdot xT = (s-r)\cdot(mx)T. \tag{21}$$

Now if m is in K, then mV is in K, since γ maps π'_∞ onto π'_∞. So $(mt)T$ is in K; define $m\phi = (mt)T$, for all m in K. Then letting $x = yt$, where y is in K, and letting m be in K, (21) implies $m\phi \cdot y\phi = (my)\phi$. Furthermore, if x and y are in K, then $(x+y)\phi = [(x+y)t]T = (xt+yt)T = x\phi + y\phi$. So ϕ is an automorphism of K.

Now let $\lambda T = \lambda a + b$, $1T = \lambda c + d$. Letting m be in K, $x = \lambda$, (21) becomes:

$$[(s-r)\cdot m\phi + r]\cdot\lambda T - r\cdot\lambda T = (s-r)\cdot(m\lambda)T,$$

or:

$$(m\lambda)T = m\phi\cdot\lambda T = \lambda a\cdot m\phi + b\cdot m\phi. \tag{22}$$

Similarly, letting m be in K and $x = 1$, (21) yields:

$$mT = m\phi\cdot 1T = \lambda c\cdot m\phi + d\cdot m\phi. \tag{23}$$

Hence, since T is an additive map, we have:

$$(\lambda x + y)T = \lambda(a\cdot x\phi + c\cdot y\phi) + (b\cdot x\phi + d\cdot y\phi). \tag{24}$$

But then T is associated with a collineation in $\mathfrak{S}\mathfrak{A}$ (see Section 3) and so we can assume that T is the identity. Then the collineation γ becomes:

$$\begin{aligned}\gamma\colon (x,y) &\to (x, (s-r)y - rx)\\ (x) &\to ((s-r)x + r)\\ [m,k] &\to [(s-r)m + r, (s-r)k]\\ [\infty,(k,0)] &\to [\infty,(k,0)].\end{aligned}$$

From this we have immediately:

$$[(s-r)m + r]x - rx = (s-r)mx. \tag{25}$$

Now if m is in K, (25) is easily seen to be satisfied; if we take $m = \lambda$, then straightforward computation from (25) leads to:

$$p - 2r = p(s-r) \tag{26}$$

$$-(r^2 - pr - q) = q(s-r)^2. \tag{27}$$

Now suppose $2 \neq 0$ in K. Then squaring both sides of (26) and dividing by (27), we are led to:

$$(r^2 - pr)(p^2 + 4q) = 0. \tag{28}$$

As above, $p^2 + 4q$ is the discriminant of $f(z)$, so is not zero, and thus (28) implies $r = 0$ or $r = p$. From this one easily deduces that $r = 0$ and $s = 1$,

or $r=p$ and $s=p-1$. But if $r=0$, $s=1$, then γ is the identity map, while if $r=p$, $s=p-1$, then γ is the involution δ (see Section 3).

On the other hand, if $2=0$ in K, then (26) and (27) become:

$$(29) \qquad p=p(s+r), \qquad r^2+pr+q=q(s+r)^2.$$

If $p\neq 0$, then $s+r=1$, and then from the second equation of (29) we have $r=0$, $s=1$, or $r=p$, $s=p+1=p-1$. So again γ is the identity or $\gamma=\delta$.

If $p=0$, then $f(z)=z^2+q$ is irreducible; since every element is a square if K is finite, K must be infinite and q a non-square. But if $p=0$, the second equation of (29) is $r^2+q=q(s+r)^2$, so $r^2=q(1+s+r)^2$. Since q is a non-square, this implies $1+s+r=0$ and $r=0$, hence $s=1$. Thus γ is the identity.

Up to a multiple by an element of $\mathfrak{L}$, every collineation can be assumed to fix the point (∞), so we have finished the first part of the theorem. The fact that $\mathfrak{S}$ and $\mathfrak{L}$ are normal in $\mathfrak{G}/\mathfrak{T}$ follows directly from an easy computation, since each normalizes the other and $\mathfrak{A}$ normalizes both of them. Alternatively, note that $\mathfrak{S}$ and $\mathfrak{L}$ are the sugroups of $\mathfrak{B}\mathfrak{S}\mathfrak{T}$ fixing pointwise the two transitive constituents on L_∞, so they must normalize each other, and it is easy to see that $\mathfrak{A}$ normalizes both.

Note that we have shown that if γ maps π'_∞ onto itself, then γ is in $\mathfrak{B}\mathfrak{S}\mathfrak{A}\mathfrak{T}$, even in the case $K=GF(3)$, or K infinite.

5. Different Hall *V*-*W* systems. In this section we will investigate the conditions under which non-isomorphic Hall V-W systems, over the same center K, lead to isomorphic planes; it is easy to see that the use of different irreducible quadratics will always lead to non-isomorphic systems. In this section we will also allow K to be infinite.

We return to equation (1) of Section 4.

$$(1) \qquad (sm-rm+r)x-rx=sk-rk,$$

where $k=m*x$, as in Section4. Letting s, r be in K in (1), we can write:

$$(2) \qquad m*x=(s-r)^{-1}[((s-r)m+r)x]-(s-r)^{-1}rx.$$

As demonstrated in Section 4, this multiplication satisfies properties (4) and (5) of Section 2, so we must consider property (6). Thus we let $m=x=\lambda$ in (2). Multiplying out, this yields:

$$\lambda*\lambda=\lambda(s-r)^{-1}(p-2r)-(s-r)^{-2}(r^2-pr-q).$$

Hence if we let $p_1 = (s-r)^{-1}(p-2r)$, $q_1 = -(s-r)^{-2}(r^2-pr-q)$, we have:

$$\lambda * \lambda = \lambda p_1 + q_1. \tag{3}$$

Since (3) does not depend on the choice of m $(=x)$, property (6) of Section 2 follows immediately. I.e., $(R, \oplus, *)$ is a Hall V-W system over the field K as center, using $f_1(z) = z^2 - p_1 z - q_1$ as the irreducible quadratic ($f_1(z)$ must be irreducible, for otherwise $(R, \oplus, *)$ would have zero-divisors; see [7]). Since the group $\mathfrak{L}$ moves (∞) anywhere in π'_∞, we have proved:

THEOREM 5.1. *Any choice of* $(\infty)'$, $(0)'$, $(1)'$ *in* π'_∞ *will lead to a Hall V-W system.*

Now we investigate a converse problem: which Hall V-W systems can be obtained in this fashion? We can always assume that $(\infty)' = (\infty)$, and so we must decide if s and r can be so chosen that

$$p_1(s-r) = p - 2r, \tag{4}$$

$$q_1(s-r)^2 = -(r^2 - pr - q), \tag{5}$$

for a given p, q, p_1, q_1, with the proviso that $f(z) = z^2 - pz - q$ and $f_1(z) = z^2 - p_1 z - q_1$ are irreducible over K.

When is $f(z)$, say, irreducible? If $2 \neq 0$ in K, then if and only if $p^2 + 4q$ is not a square, as is well-known. But if $2 = 0$, we have no such condition. We will develop one of a strikingly similar sort, one which appears to be vaguely known, but does not seem to be in the literature. Let K be a field (finite or infinite) of characteristic two and let $P(K)$ be the set of elements in K which can be written as $x^2 + x$, for some x in K.

LEMMA 5.1. *If* $2 = 0$ *in* K, *then* $P = P(K)$ *is an additive subgroup of* $(K, +)$, *and if* K *is finite,* P *contains exactly half of the elements of* K. *Furthermore, the quadratic* $az^2 + bz + c$ *(where* $a \neq 0$*) is irreducible over* K *if and only if* (i) $b \neq 0$ *and* ca/b^2 *is not in* P, *or* (ii) K *is imperfect,* $b = 0$, *and* c/a *is not a square in* K. *Finally, the irreducible quadratics* $az^2 + bz + c$ *and* $a_1 z^2 + b_1 z + c_1$ *define the same quadratic extension fields of* K *if and only if* (iii) $b \neq 0$, $b_1 \neq 0$, *and* $ca/b^2 + c_1 a_1/b_1^2$ *is in* P, *or* (iv) K *is imperfect,* $b = b_1 = 0$ *and* $x^2 c/a + y^2 c_1/a_1$ *is a square for some non-zero* x *and* y *in* K.

Proof. The first sentence is easy to prove. The second part depends on noting that $az^2 + bz + c = (b^2/a)[(az/b)^2 + (az/b) + (ca/b^2)]$ if $b \neq 0$, so $az^2 + bz + c = 0$ for some z in K if and only if $ca/b^2 = (az/b)^2 + (az/b)$.

I.e., ca/b^2 is in P. The rest of the proof is straightforward computation, which we omit.

Note that if we only consider perfect fields of characteristic two, then conditions (ii) and (iv) are superfluous, and the analogy with the discriminant becomes clearer. In general, if $2=0$ in K and if $b\neq 0$, we shall call ac/b^2 the discriminant of the expression az^2+bz+c.

Now we return to (4) and (5). Squaring (4) and dividing by (5), we have:

$$r^2(p_1^2+4q_1)-pr(p_1^2+4q_1)+p^2q_1-p_1^2q=0. \tag{6}$$

Thinking of (6) as a quadratic equation for r, its discriminant, if $2\neq 0$, is $\Delta=p_1^2\delta\delta_1$, where $\delta=p^2+4q$, $\delta_1=p_1^2+4q_1$. Then Δ is a square if and only if $p_1=0$ or $\delta\delta_1$ is a square. But $\delta\delta_1$ is a square if and only if the quadratic extension fields defined over K by $f(z)$ and $f_1(z)$ are the same; if $p_1\neq 0$ we can solve for s if we can solve (6) for r. On the other hand, if $p_1=0$, then (4) implies $2r=p$, and then (5) becomes:

$$(s-r)^2=(r^2+q)/q_1=\delta/\delta_1, \tag{7}$$

and we can solve for s if and only if δ/δ_1 is a square. But this is equivalent to $\delta\delta_1$ being a square, and again, we are reduced to the case that $f(z)$ and $f_1(z)$ define the same quadratic extension field of K.

Now if $2=0$ in K, (6) becomes:

$$r^2p_1^2+pp_1^2r+p^2q_1+p_1^2q=0. \tag{8}$$

If $p\neq 0$, $p_1\neq 0$, then the discriminant of (8) is quickly computed to be $\Delta=\delta+\delta_1$, where $\delta=q/p^2$, $\delta_1=q_1/p_1^2$. So (8) can be solved for r if and only if Δ is in $P(K)$, which is to say, if and only if $f(z)$ and $f_1(z)$ define the same quadratic extension field of K; and of course we can solve for s if we can solve for r.

If $p=0$, $p_1\neq 0$, then (8) becomes $r^2+q=0$, but this is presumably without solutions, since $f(z)$ is irreducible, and so (8) cannot be solved. But also the extension fields defined by $f(z)$ and $f_1(z)$ are not isomorphic in this case. If $p\neq 0$, $p_1=0$, then (8) becomes $p^2q_1=0$, which is impossible, so we have a similar situation.

Finally, if $p=p_1=0$, then (8) gives no information, so we return to (5), which yields:

$$q_1(s+r)^2=r^2+q. \tag{9}$$

This is solvable for s and r if and only if $(r^2+q)/q_1$ is a square. If such

an s and r exist, then letting $x=s+r$, $y=1$, $z=r$ gives $x^2q_1+y^2q=z^2$. Conversely, if $x^2q_1+y^2q=z^2$ for non-zero x, y, z in K, then we let $s+r=x/y$, $r=z/y$. So, utilizing Lemma 5.1, (9) is solvable if and only if $f(z)$ and $f_1(z)$ define the same quadratic extension field of K.

THEOREM 5.2. *If $f(z)$ and $f_1(z)$ are irreducible quadratics over K, then the Hall V-W planes defined by $f(z)$ and $f_1(z)$ are isomorphic if $f(z)$ and $f_1(z)$ have zeros in the same quadratic extension field of K.*[4]

COROLLARY. *Two finite Hall V-W systems of the same order define isomorphic projective planes.*

The corollary is of course immediate since there is only one finite field of any given order. Theorem 5.2 probably has a converse, but the detailed investigation of moving the point (∞) is necessary, and this is extremely tedious.

6. The case $K=GF(3)$. Throughout this section we restrict attention to $K=GF(3)$; in view of the corollary to Theorem 5.2, we need consider only one Hall V-W system. So we let $p=0$, $q=-1$, and then the V-W system R is even a near-field; i.e., the multiplication is associative. We shall determine what collineations, besides those of Section 3, π possesses. To begin with, let $\mathfrak{N}$ be the group defined as follows. For each t in R, $t\neq 0$, define θ_t by:

$$\theta_t\colon (x,y)\to(x,ty) \qquad [m,k]\to[tm,tk]$$
$$(x)\to(tx) \qquad [\infty,(k,0)]\to[\infty,(k,0)],$$

where (∞) and L_∞ are fixed. Then $\mathfrak{N}$ is a collineation group, and taken with the groups of Section 3, it is clear that $\mathfrak{G}$ is transitive on the points of L_∞.

André has discovered ([1]) that for each point P on L_∞ there is a uniquely defined point $P'\neq P$ such that $(P')'=P$, and such that any collineation of π must map a pair (P,P') onto a pair (Q,Q'). André's results are not stated in this fashion, but the properties of the "zulässige Punktepaare" of [1] are easily seen to force this conclusion. Thus the pairs (P,P') are systems of imprimitivity on L_∞.

[4] In some recent papers (Rivista Mat. Univ. Parma, vol. 8 (1957); Convegno Internazionale Reticoli e Geometrie Proiettive, (1957)) and in a paper to appear in Rendiconti dell'Accademia Nazionale dei Lincei, Gianfranco Panella has investigated the conditions under which two Hall V-W systems give isomorphic planes, and has obtained results cast in somewhat different form than ours.

LEMMA 6.1. *If $P = (\infty)$, then $P' = (0)$, and if $P = (m) \neq (0)$, then $P' = (-m)$.*

The proof of Lemma 6.1 can be found in [1], although it is easy to use Section 3 to give a proof, using the fact that the pairs exist.

Now let $\mathfrak{G}_1$ be the collineation group of π generated by the groups of Section 3 and the group $\mathfrak{N}$. Let $\bar{\mathfrak{G}}_1$ be the restriction of $\mathfrak{G}_1$ (as a permutation group) to the imprimitive systems (P, P') on L_∞, so that $\bar{\mathfrak{G}}_1$ is a permutation group of degree 5. We note that $\mathfrak{G}_1$ is a subgroup of $\mathfrak{G}$ and that $\bar{\mathfrak{G}}_1$ is a homomorphic image of $\mathfrak{G}_1$, so if we show that $\bar{\mathfrak{G}}_1$ is non-solvable, the same result will hold for $\mathfrak{G}$.

LEMMA 6.2. *$\bar{\mathfrak{G}}_1$ contains a transposition.*

Proof. The collineation $\zeta(1,1)$ in $\mathfrak{L}$ fixes every point (x), x not in K, and interchanges the pair $((\infty), (0))$ with the pair $((1), (-1))$. So in $\bar{\mathfrak{G}}_1$ $\zeta(1,1)$ induces a transposition.

LEMMA 6.3. *$\bar{\mathfrak{G}}_1$ is doubly transitive on its five symbols.*

Proof. The collineations of $\mathfrak{N}$ fix the pair $((\infty), (0))$ and are transitive on the remaining points of L_∞; hence they are certainly transitive on the pairs $(P, P') \neq ((\infty), (0))$. Since $\mathfrak{G}_1$ is transitive on the pairs (P, P'), this implies that $\bar{\mathfrak{G}}_1$ is transitive on its five symbols and the subgroup fixing one symbol is transitive on the remaining four; thus $\mathfrak{G}_1$ is doubly transitive.

THEOREM 6.1. *$\mathfrak{G}$ is non-solvable.*

Proof. As remarked above, it suffices to show that $\bar{\mathfrak{G}}_1$ is non-solvable. But $\bar{\mathfrak{G}}_1$ is doubly transitive and contains a transposition, so it is isomorphic to the symmetric group on five symbols, and thus is non-solvable.

We have now shown that the collineation group of any Hall V-W plane is non-solvable, even though we have not determined all of the group (perhaps) for the infinite planes of the class.

Let us study the group $\mathfrak{G}$ a little more for this case $K = GF(3)$. We suppose γ is in $\mathfrak{G}$; up to a multiple by an element in $\mathfrak{N}\mathfrak{L}$, we can assume that γ fixes (∞), and from André's result ([1]), a collineation which fixes (∞) also fixes (0). Again up to a multiple by an element of $\mathfrak{N}$, we can assume that (1) is fixed (and thus (-1) is fixed); because of $\mathfrak{T}$, $(0, 0)$ can be assumed to be fixed. Then from the remark at the end of Theorem 4.2, our collineation is already contained in $\mathfrak{S}$ (for $K = GF(3)$, $\mathfrak{A}$ clearly has order one). Thus:

THEOREM 6.2. $\mathfrak{G}_1 = \mathfrak{G}$.

Indeed, one can also show that the order of $\mathfrak{G}$ is $10 \cdot 81 \cdot 48 \cdot 8$, since the subgroup fixing $(0,0)$ and (∞) is $\mathfrak{S}\mathfrak{N}$, of order $48 \cdot 8$; the involution δ of Section 3 is equal to the element θ_{-1} of $\mathfrak{N}$. (And $\mathfrak{S}\mathfrak{N}$ is a group, for $\theta_t\sigma(S) = \sigma(S)\theta_{(ts)S}$.) The determination of the group $\mathfrak{G}$, as well as its order, was already carried out by André in [1], by the way.

Finally, it is easy to show that for any Hall V-W plane, the collineation group is doubly transitive on finite points if and only if it is transitive on the points of L_∞. Hence for the finite planes of the class, the plane of order nine is the only one whose group is doubly transitive on finite points.

THE OHIO STATE UNIVERSITY
AND
UNIVERSITY OF CHICAGO.

REFERENCES.

[1] Johannes André, "Projektive Ebenen über Fastkörpern," *Mathematische Zeitschrift*, vol. 62 (1955), pp. 137-160.

[2] Marshall Hall, Jr., "Projective planes," *Transactions of the American Mathematical Society*, vol. 54 (1943), pp. 229-277.

[3] D. R. Hughes, "Planar division neo-rings," *ibid.*, vol. 80 (1955), pp. 502-527.

[4] ———, "Partial difference sets," *American Journal of Mathematics*, vol. 78 (1956), pp. 650-674.

[5] ———, "A class of non-Desarguesian projective planes," *Canadian Journal of Mathematics*, vol. 9 (1957), pp. 378-388.

[6] ———, "A note on some partially transitive projective planes," *Proceedings of the American Mathematical Society*, vol. 8 (1957), pp. 978-981.

[7] Günter Pickert, *Projektive Ebenen*, Berlin, 1955.

[8] B. L. van der Waerden, *Gruppen von Linearen Transformationen*, New York, 1948.

[9] Guido Zappa, "Sui gruppi di collineazioni dei piani di Hughes," *Bolletino della Unione Matematica Italiana*, vol. 12 (1957), pp. 507-516.

A PARTITION FUNCTION WITH SOME CONGRUENCE CONDITION.*

By Shô Iseki.

Introduction. It is well known that the number $p(n)$ of unrestricted partitions of a positive integer n can be expressed by a convergent series (see [9]).

In this paper we shall be concerned with the number $p(n;a,M)$ of partitions of n into positive summands congruent to $\pm a$ modulo M, where a, M are integers with $M \geqq 2$.

This partition function $p(n;a,M)$ has been treated for certain special values of M; namely, $M=2$ by Hua [2], $M=5$ by Lehner [5], $M=6$ by Niven [8], and $M=p$ (p a prime >3) by Livingood [6]; a convergent series representation of $p(n;a,M)$ being obtained in each case.

The main object of the present paper is to derive a convergent series for $p(n;a,M)$ in which M assumes *general* values.

We may suppose without loss of generality that $0<a<M$, $(a,M)=1$; for in the case where $a=0$ and $M \mid n$, the partition function in question reduces trivially to $p(n/M)$, while in the case where $d=(a,M)>1$ and $d \mid n$, it reduces to $p(n/d;a/d,M/d)$. Further we remark that the case $M=2$ (partitions into odd summands) is equivalent to the case $M=4$, i.e., $p(n;1,2)=p(n;1,4)$. Consequently it suffices to consider the case $M \geqq 3$.

We apply the Hardy-Ramanujan method with modifications due to Rademacher [10]. In order to utilize this method, however, it is necessary to solve the following two subsidiary problems:

The first problem is to find a suitable transformation equation for the generating function of $p(n;a,M)$. The usual method of contour integration seems to be rather complicated in our case. However, we can show, in a simple way, the existence of the transformation equation, the proof of which being based on a certain functional equation recently obtained by the author [3]. This will be done in Section 1 of this paper.

The second is to get a non-trivial estimate for a certain exponential sum which is introduced as a consequence of the transformation equation. We shall

* Received February 9, 1959.

discuss this problem in Section 2. The analysis used is somewhat elaborate, but we can reduce the sum to a generalized Kloosterman sum, for which suitable estimates are known. To achieve this result we follow partly a method due to Lehner [5]. But Lehner's original method seems to be effective only for the case $(6, M)=1$. We therefore have to make a partial revision of his method to secure the case $(6, M)>1$.

We shall derive the desired series expansion in Section 3, by making use of the results of Sections 1 and 2.

The final section is devoted to the investigation of some asymptotic properties of $p(n; a, M)$ which are deducible from the series representation.

The author wishes to express his gratitude to Professor Joseph Lehner for kind information on the literature.

1. The transformation equation. The generating function of $p(n; a, M)$ is found to be, for $M \geqq 3$,

$$F(x; a, M)=1+\sum_{n=1}^{\infty} p(n; a, M) x^{n}=\prod_{m=0}^{\infty}(1-x^{mM+a})^{-1}\ (1-x^{mM+M-a})^{-1},$$

where x is a complex variable with $|x|<1$.

Now let h, k be coprime integers with $k \geqq 1$. Denote by D and K the g.c.d. and the l.c.m. of k and M respectively. Put $k=k_1 D$, $M=m_1 D$, so that $(k_1, m_1)=1$, and choose any integers γ, δ satisfying

$$\gamma k_1-\delta m_1=1. \tag{1.1}$$

Let, then, H be any fixed solution of the congruence [1]

$$hH \equiv \delta \pmod{k}. \tag{1.2}$$

Furthermore we write

$$x=\exp(2\pi ih/k-2\pi z/k); \qquad x'=\exp(2\pi iH/k-2\pi/Kz), \tag{1.3}$$

where z is a complex variable with $\Re(z)>0$. Define

$$F(x'; b, D, \rho)=\prod_{m=0}^{\infty}(1-\rho x'^{mD+b})^{-1}\ (1-\rho^{*} x'^{mD+D-b})^{-1} \tag{1.4}$$

with the notations

$$b=ha-D[ha/D], \quad \rho=\exp(-2\pi i\gamma a/M), \quad \rho^{*}=\exp(2\pi i\gamma a/M), \tag{1.5}$$

[1] In the case $(k, M)=M$, we have $m_1=1$. Hence we may choose $\gamma=0$, $\delta=-1$ in (1.1). Then (1.2) becomes $hH \equiv -1 \pmod{k}$. This congruence has been used by Lehner [5] and Livingood [6].

in which $[t]$ denotes the greatest integer not exceeding t. (Note that $b \equiv ha \pmod{D}$, $0 \leqq b < D$, $(b, D) = 1$; $\rho^* = \rho^{-1}$.)

Then there exists a transformation equation which connects $F(x; a, M)$ with $F(x'; b, D, \rho)$, and therefore exhibits the asymptotic behavior of $F(x; a, M)$ near its singularity at each rational point on the unit circle.

THEOREM 1.[2] *Let*

$$\omega(h, k) = \exp\{2\pi i \sigma(h, k)\},$$
$$\sigma(h, k) = \sum_{\mu} (\mu/K - \tfrac{1}{2})(h\mu/k - [h\mu/k] - \tfrac{1}{2}), \tag{1.6}$$

where μ runs over the integers $a, M + a, 2M + a, \cdots, (k_1 - 1)M + a$; and set

$$A = 6a^2 - 6Ma + M^2, \qquad B = 6b^2 - 6Db + D^2. \tag{1.7}$$

Then, if $M \geqq 3$, we have the transformation equation

$$F(x; a, M) = \omega(h, k) \exp\{(\pi/6Mk)(B/z - Az)\} F(x'; b, D, \rho). \tag{1.8}$$

To prove Theorem 1 we need the following lemma.

LEMMA 1. *If μ runs over the integers*

$$a, M + a, 2M + a, \cdots, (k_1 - 1)M + a,$$

then $\mu^* = h\mu - k[h\mu/k]$ runs, in some order, over the integers

$$b, D + b, 2D + b, \cdots, (k_1 - 1)D + b.$$

Proof. First, it is easy to see that the assumed values of μ are k_1 integers which are mutually incongruent modulo k, and hence, observing that $\mu^* \equiv h\mu \pmod{k}$ and $(h, k) = 1$, it follows that the values of μ^* are distinct k_1 integers of the interval $0 \leqq \mu^* < k$.

Next, the facts that $\mu^* \equiv h\mu \pmod{k}$ and that $\mu \equiv a \pmod{M}$ together yield $\mu^* \equiv ha \pmod{D}$, so that $\mu^* \equiv b \pmod{D}$ since $ha \equiv b \pmod{D}$.

On the other hand, any integer μ^* satisfying both $0 \leqq \mu^* < k$ and $\mu^* \equiv b \pmod{D}$ must be one of the integers $b, D + b, 2D + b, \cdots, (k_1 - 1)D + b$ since $0 \leqq b < D$ and $k_1 D = k$. But these are exactly k_1 integers. Thus our lemma is proved.

---

[2] The case $D = 1$ of Theorem 1 can also be expressed in a different form, see [4], Theorem 2.

Proof of Theorem 1. We apply the following functional equation ([3], p. 654, Theorem 1):

$$\begin{aligned}(1.9)\qquad &\sum_{l=0}^{\infty}\{\lambda((l+\alpha)z-i\beta)+\lambda((l+1-\alpha)z+i\beta)\}+\pi z(\alpha^2-\alpha+\tfrac{1}{6})\\ &=\sum_{l=0}^{\infty}\{\lambda((l+\beta)/z+i\alpha)+\lambda((l+1-\beta)/z-i\alpha)\}\\ &\qquad+(\pi/z)(\beta^2-\beta+\tfrac{1}{6})+2\pi i(\alpha-\tfrac{1}{2})(\beta-\tfrac{1}{2}),\end{aligned}$$

where $0<\alpha<1$, $0\leqq\beta\leqq 1$ (or $0\leqq\alpha\leqq 1$, $0<\beta<1$), $\Re(z)>0$, and $\lambda(t)$ denotes $-\log(1-e^{-2\pi t})$, the logarithm having its principal value.

Let us put

$$(1.10)\qquad \alpha=\mu/K,\qquad \beta=\mu^*/k,$$

where μ, μ^* are those of Lemma 1, so that we have $0<\alpha<1$, $0\leqq\beta<1$, since $0<\mu<k_1M=K$ and $0\leqq\mu^*<k$. Substituting (1.10) into (1.9) and replacing z by m_1z, the left member of (1.9) becomes

$$\begin{aligned}(1.11)\qquad &\sum_{l=0}^{\infty}\{\lambda((l+\mu/K)m_1z-i\mu^*/k)+\lambda((l+1-\mu/K)m_1z+i\mu^*/k)\}\\ &\qquad+\pi m_1z\{(\mu/K)^2-\mu/K+\tfrac{1}{6}\}\\ &=\sum_{l=0}^{\infty}\{\lambda((Kl+\mu)(z-ih)/k)+\lambda((Kl+K-\mu)(z-ih)/k)\}\\ &\qquad+\pi m_1z\{(\mu/K)^2-\mu/K+\tfrac{1}{6}\},\end{aligned}$$

since $K=m_1k$ and $\mu^*/k\equiv h\mu/k \pmod 1$; while the right member of (1.9) becomes

$$\begin{aligned}(1.12)\qquad &\sum_{l=0}^{\infty}\{\lambda((l+\mu^*/k)/m_1z+i\mu/K)+\lambda((l+1-\mu^*/k)/m_1z-i\mu/K)\}\\ &\qquad+(\pi/m_1z)\{(\mu^*/k)^2-\mu^*/k+\tfrac{1}{6}\}+2\pi i(\mu/K-\tfrac{1}{2})(\mu^*/k-\tfrac{1}{2})\\ &=\sum_{l=0}^{\infty}\{\lambda((kl+\mu^*)/Kz+i\mu/K)+\lambda((kl+k-\mu^*)/Kz-i\mu/K)\}\\ &\qquad+(\pi/m_1z)\{(\mu^*/k)^2-\mu^*/k+\tfrac{1}{6}\}+2\pi i(\mu/K-\tfrac{1}{2})(\mu^*/k-\tfrac{1}{2}).\end{aligned}$$

Now, it follows from the congruence $\mu^*\equiv h\mu \pmod k$ and (1.2) that $H\mu^*\equiv hH\mu\equiv\delta\mu \pmod k$, and so

$$(1.13)\qquad m_1H\mu^*\equiv m_1\delta\mu\ (\mathrm{mod}\ m_1k=K).$$

On the other hand, $\mu\equiv a \pmod M$ implies

$$(1.14)\qquad \gamma k_1\mu\equiv\gamma k_1a\ (\mathrm{mod}\ k_1M=K).$$

It follows from (1.13), (1.14) and (1.1) that

$$\mu\equiv -m_1H\mu^*+\gamma k_1a \pmod K$$

and hence, noting that $K = m_1 k = k_1 M$, we have

$$
(1.15)\qquad \begin{aligned} \mu/K &\equiv -m_1 H\mu^*/K + \gamma k_1 a/K \pmod 1 \\ &= -H\mu^*/k + \gamma a/M. \end{aligned}
$$

Therefore the right member of (1.12) transforms into the form

$$
(1.16)\qquad \begin{aligned} &\sum_{l=0}^{\infty} \{\lambda((kl+\mu^*)(1/Kz - iH/k) + i\gamma a/M) \\ &\quad + \lambda((kl+k-\mu^*)(1/Kz - iH/k) - i\gamma a/M)\} \\ &\quad + (\pi/m_1 z)\{(\mu^*/k)^2 - \mu^*/k + \tfrac{1}{6}\} + 2\pi i(\mu/K - \tfrac{1}{2})(\mu^*/k - \tfrac{1}{2}). \end{aligned}
$$

Equating the right-hand side of (1.11) with (1.16), adding up the result over $\mu = a, M+a, 2M+a, \cdots, (k_1 - 1)M + a$, and using Lemma 1, we get

$$
(1.17)\qquad \begin{aligned} &\sum_{m=0}^{\infty} \{\lambda((mM+a)(z-ih)/k) + \lambda((mM+M-a)(z-ih)/k)\} \\ &\qquad\qquad + \pi m_1 z \sum_{\mu} \{(\mu/K)^2 - \mu/K + \tfrac{1}{6}\} \\ &= \sum_{m=0}^{\infty} \{\lambda((mD+b)(1/Kz - iH/k) + i\gamma a/M) \\ &\quad + \lambda((mD+D-b)(1/Kz - iH/k) - i\gamma a/M)\} \\ &\quad + (\pi/m_1 z) \sum_{\mu} \{(\mu^*/k)^2 - \mu^*/k + \tfrac{1}{6}\} + 2\pi i \sum_{\mu} (\mu/K - \tfrac{1}{2})(\mu^*/k - \tfrac{1}{2}). \end{aligned}
$$

Here we have

$$
(1.18)\qquad \sum_{\mu} \{(\mu/K)^2 - \mu/K + \tfrac{1}{6}\} = (6a^2 - 6Ma + M^2)/6MK = A/6MK
$$

by (1.7), and similarly

$$
(1.19)\qquad \sum_{\mu} \{(\mu^*/k)^2 - \mu^*/k + \tfrac{1}{6}\} = (6b^2 - 6Db + D^2)/6Dk = B/6Dk.
$$

It is now obvious that the desired equation (1.8) follows from (1.17), (1.18) and (1.19).

This completes the proof of Theorem 1.

2. Estimation of some exponential sum. The transformation equation (1.8) contains the complicated root of unity $\omega(h,k)$ whose definition appears in (1.6).

We shall first express $\omega(h,k)$ in a more elementary form than (1.6), without making use of the function $[t]$.

Writing $\mu^* = h\mu - k[h\mu/k]$, we have from (1.6)

$$
(2.1)\qquad \begin{aligned} \sigma(h,k) &= \sum_{\mu} (\mu/K - \tfrac{1}{2})(\mu^*/k - \tfrac{1}{2}) \\ &= \sum_{\mu} (\mu/K)(\mu^*/k - \tfrac{1}{2}) - \tfrac{1}{2} \sum_{\mu} (\mu^*/k - \tfrac{1}{2}). \end{aligned}
$$

Here, clearly

$$(2.2)\qquad \begin{aligned}\sum_\mu (\mu/K)(\mu^*/k-\tfrac{1}{2}) &= \sum_\mu (\mu/K)(h\mu/k-[h\mu/k]-\tfrac{1}{2})\\ &= (h/Kk)\sum_\mu \mu^2-(1/K)\sum_\mu \mu[h\mu/k]-(1/2K)\sum_\mu \mu,\end{aligned}$$

and further

$$(2.3)\qquad \begin{aligned}\sum_\mu \mu &= \sum_{l=0}^{k_1-1}(a+Ml) = ak_1+\tfrac{1}{2}Mk_1(k_1-1),\\ \sum_\mu \mu^2 &= \sum_{l=0}^{k_1-1}(a+Ml)^2 = a^2k_1+aMk_1(k_1-1)\\ &\qquad +\tfrac{1}{6}M^2k_1(k_1-1)(2k_1-1).\end{aligned}$$

Also, by Lemma 1,

$$(2.4)\qquad \begin{aligned}\sum_\mu (\mu^*/k-\tfrac{1}{2}) &= \sum_{l=0}^{k_1-1}((b+Dl)/k-\tfrac{1}{2})\\ &= bk_1/k+Dk_1(k_1-1)/2k-\tfrac{1}{2}k_1 = b/D-\tfrac{1}{2}.\end{aligned}$$

It follows from (2.1), (2.2), (2.3) and (2.4) that

$$(2.5)\qquad \begin{aligned}12Mk\sigma(h,k) &= 2h\{6a^2+6aM(k_1-1)+M^2(k_1-1)(2k_1-1)\}\\ &\quad -3k\{2a+M(k_1-2)+2bm_1\}-12D\sum_\mu \mu[h\mu/k].\end{aligned}$$

Hence $12Mk\sigma(h,k)$ is always an integer. Moreover

$$(2.6)\qquad \sum_\mu \mu[h\mu/k] = \sum_{l=0}^{k_1-1}(a+Ml)[h\mu/k] = a\sum_\mu [h\mu/k]+M\sum_{l=0}^{k_1-1} l[h\mu/k] \qquad (\mu=a+Ml),$$

and

$$(2.7)\qquad \begin{aligned}\sum_\mu [h\mu/k] = \sum_\mu (h\mu/k-\mu^*/k) &= (h/k)\{ak_1+\tfrac{1}{2}Mk_1(k_1-1)\}\\ &\quad -(1/k)\{bk_1+\tfrac{1}{2}Dk_1(k_1-1)\}.\end{aligned}$$

From (2.5), (2.6) and (2.7) we obtain

$$\begin{aligned}12Mk\sigma(h,k) &= 2hM\{3a(k_1-1)+M(k_1-1)(2k_1-1)\}\\ &\quad -3K(k+2b-2D)+6a(2b-D)-12DM\sum_{l=0}^{k_1-1} l[h\mu/k].\end{aligned}$$

Multiplying both sides by $\gamma/12DM$ (γ being given in (1.1)), we deduce

$$(2.8)\qquad \begin{aligned}\gamma k_1\sigma(h,k) &\equiv (\gamma h/k)(aX+MY)-(\gamma k_1/4D)(k+2b-2D)\\ &\quad +(a\gamma/2DM)(2b-D) \pmod 1,\end{aligned}$$

where X, Y are integers defined by

$$(2.9)\qquad X=\tfrac{1}{2}k_1(k_1-1), \qquad Y=\tfrac{1}{6}k_1(k_1-1)(2k_1-1).$$

Now from (2.5) we see that

$$12Mk\sigma(h,k) \equiv 2hM^2(k_1-1)(2k_1-1) \pmod 3.$$

Here if $3 \nmid k$, then $3 \nmid k_1$ and so we have

(2.10) $$12Mk\sigma(h,k) \equiv 0 \pmod 3 \text{ if } 3 \nmid k.$$

Next, from (2.5),

$$\begin{aligned}12Mk\sigma(h,k) &\equiv 2hM^2(k_1-1)(2k_1-1) - 3k\{2a + M(k_1-2) + 2bm_1\}\\ &\equiv 2hM^2(k_1-1)(2k_1-1) + k(2a + m_1k + 2M + 2bm_1) \pmod 4.\end{aligned}$$

Here if $2 \nmid k$, then $2 \nmid k_1$ and therefore, noting that $k^2 \equiv 1 \pmod 4$ and that

$$k(2a + 2M + 2bm_1) \equiv 2a + 2M + 2bm_1 \pmod 4,$$

we have

(2.11) $$12Mk\sigma(h,k) \equiv 2a + 2M + (2b+1)m_1 \pmod 4 \text{ if } 2 \nmid k.$$

We now introduce two integers f, g defined as follows:

(2.12) $$\begin{aligned} f&=12, & g&=1 && \text{for } (k,6)=1,\\ f&=3, & g&=4 && \text{for } (k,6)=2,\\ f&=4, & g&=3 && \text{for } (k,6)=3,\\ f&=1, & g&=12 && \text{for } (k,6)=6.\end{aligned}$$

Then we see that $fg = 12$ and $(f,k) = 1$ in all cases. In addition, any prime in g divides k, so that $(h,k) = 1$ implies

(2.13) $$(h, gDk) = 1,$$

and $(f,k) = 1$ implies

(2.14) $$(f, gDk) = 1.$$

Furthermore, examination of (2.10), (2.11) and (2.12) yields

(2.15) $$12Mk\sigma(h,k) \equiv 6a + 6M + 3(2b-1)m_1 \pmod f.$$

We next have, on the one hand,

$$\sum_\mu (\mu^*/k - \tfrac{1}{2})^2 = \sum_\mu (\mu^*/k)^2 - \sum_\mu (\mu^*/k) + \tfrac{1}{4}\sum_\mu 1$$

which reduces after simplification to

(2.16) $$(B - k^2)/6Dk + k_1/4,$$

where B is given in (1.7); while, on the other hand,

$$\begin{aligned}\sum_\mu (\mu^*/k-\tfrac12)^2 &= \sum_\mu (h\mu/k-[h\mu/k]-\tfrac12)^2 = 2h\sum_\mu (\mu/k)(\mu^*/k-\tfrac12)\\ &\quad -(h/k)^2\sum_\mu \mu^2+\sum_\mu [h\mu/k]([h\mu/k]+1)+\tfrac14\sum_\mu 1\\ &= 2hm_1\sigma(h,k)+hm_1(b/D-\tfrac12)\\ &\quad -(h^2/6Dk)\{2K^2+3K(2a-M)+A\}+2S+k_1/4.\end{aligned} \tag{2.17}$$

where we have made use of (2.1), (2.4) and (2.3); A is given in (1.7), and S is an integer defined by

$$S=\tfrac12\sum_\mu [h\mu/k]([h\mu/k]+1).$$

Comparing (2.16) and (2.17) yields

$$\begin{aligned}12Mhk\sigma(h,k) &= h^2\{2K^2+3K(2a-M)+A\}+(B-k^2)\\ &\quad +3hkm_1(D-2b)-12DkS.\end{aligned} \tag{2.18}$$

Let us now assume that H is any fixed solution of the congruence (cf. (1.2))

$$hH\equiv\delta \pmod{gDk}, \tag{2.19}$$

which is solvable by virtue of (2.13). Multiplying (2.18) by this H, and observing that $gDk \mid 12Dk$, we obtain

$$12Mk\delta\sigma(h,k)\equiv uh+vH+3\delta km_1(D-2b) \pmod{gDk}, \tag{2.20}$$

where

$$u=\delta\{2K^2+3K(2a-M)+A\},\qquad v=B-k^2. \tag{2.21}$$

We take here any integers ϕ, ψ satisfying

$$f\phi+gDk\psi=1, \tag{2.22}$$

which is possible in view of (2.14). Then, recalling that $fg=12$, we deduce from (2.15), (2.20) and (2.22) that

$$\begin{aligned}12Mk\delta\sigma(h,k) &\equiv f\phi\{uh+vH+3\delta km_1(D-2b)\}\\ &\quad +gDk\psi\delta\{6a+6M+3(2b-1)m_1\} \pmod{12Dk}.\end{aligned}$$

Dividing both sides by $12Dk$, we have

$$\begin{aligned}\delta m_1\sigma(h,k) &\equiv (\phi/gDk)(uh+vH)+(3\phi\delta m_1/gD)(D-2b)\\ &\quad +(g\psi\delta/4)\{2a+2M+(2b-1)m_1\} \pmod 1.\end{aligned} \tag{2.23}$$

It now follows from (2.8), (2.23) and (1.1) that

$$(2.24)\quad \begin{aligned}\sigma(h,k) &\equiv (1/gDk)(\{gD\gamma(aX+MY)-\phi u\}h-\phi vH)\\ &\quad-(\gamma k_1/4D)(k+2b-2D)+\{(a\gamma/2DM)+(3\phi\delta m_1/gD)\}(2b-D)\\ &\quad-(g\psi\delta/4)\{2a+2M+(2b-1)m_1\} \pmod 1\\ &=(1/gDk)(Uh+VH)+W,\end{aligned}$$

say. We remark here that U and V are integers, U being independent of h, and that if we keep b fixed and restrict h by the congruence $ah\equiv b \pmod D$ (see (1.5)), then V, W are also independent of such restricted values of h.

From (1.6) and (2.24) we obtain the desired expression:

$$(2.25)\qquad \omega(h,k)=\exp\{(2\pi i/gDk)(Uh+VH)+2\pi iW\}.$$

We now proceed to consider the following exponential sum:

$$(2.26)\qquad S_k=S_k(n,\nu;b,D;s_1,s_2)=\sum_h{}' \omega(h,k)\exp\{2\pi i(-nh+\nu H)/k\}$$
$$(h \bmod k,\ ah\equiv b \pmod D),\ s_1\leqq(\bar h)<s_2).$$

Here n, ν, b, s_1, s_2 are all integers with $n\geqq 0$, $0\leqq b<D$, $(b,D)=1$, $0<s_2-s_1\leqq k$; H is defined by (1.2); $\bar h$ is any fixed solution of $h\bar h\equiv 1 \pmod k$; the notation $s_1\leqq(\bar h)<s_2$ means that there exists an integer t such that $t\equiv\bar h \pmod k$, $s_1\leqq t<s_2$; and the summation symbol $\sum'_h$ denotes here and subsequently that h runs over any reduced residue system of the given modulus with certain summation conditions indicated in parentheses.

First, we notice that each summand in S_k has a period k with respect to h, and hence the residue system modulo k over which the summation extends can be arbitrary.

Let us now define an arithmetic function $f(s)$ by

$$(2.27)\qquad f(s)=\begin{cases}1, & \text{if } s_1\leqq(s)<s_2,\\ 0, & \text{otherwise.}\end{cases}$$

Then $f(s)$ is a periodic function with period k, so that it permits of expansion into a finite Fourier series of the form

$$(2.28)\qquad f(s)=\sum_{l=0}^{k-1} c_l\exp(2\pi isl/k).$$

Here

$$c_l=k^{-1}\sum_{s \bmod k} f(s)\exp(-2\pi isl/k)=k^{-1}\sum_{s=s_1}^{s_2-1}\exp(-2\pi isl/k),$$

and so

$$c_0=(s_2-s_1)/k,$$

$$c_l=\csc(\pi l/k)\exp(\pi il/k)\{\exp(-2\pi is_1l/k)-\exp(-2\pi is_2l/k)\}/2ik \qquad (l\neq 0)$$

hence we have

$$(2.29)\qquad \begin{aligned}&|c_0|\leqq 1,\\ &|c_l|\leqq \csc(\pi l/k)/k\leqq \begin{cases}1/2l & (1\leqq l\leqq k/2),\\ 1/2(k-l) & (k/2\leqq l\leqq k-1).\end{cases}\end{aligned}$$

By (2.27), we may write

$$(2.30)\qquad S_k=\sum_h{}' f(\bar h)\,\omega(h,k)\exp\{2\pi i(-nh+\nu H)/k\} \qquad (h \bmod k,\ ah\equiv b \pmod D)).$$

Further, it is easy to see that the value of S_k is not affected by the selection of $\bar h$ and H as solutions of their congruences. Accordingly, we may employ those $\bar h$, H which satisfy

$$h\bar h\equiv 1 \pmod{gDk}, \qquad hH\equiv\delta \pmod{gDk}$$

(see (2.19)), respectively. Then we have

$$(2.31)\qquad H\equiv\delta\bar h \pmod{gDk}$$

and *a fortiori*

$$(2.32)\qquad H\equiv\delta\bar h \pmod{k}.$$

From (2.28), (2.30), (2.32) and the periodicity of the summands it follows that

$$\begin{aligned}S_k&=\sum_{l=0}^{k-1}c_l\sum_h{}'\omega(h,k)\exp(2\pi i\{-nh+(\nu\delta+l)\bar h\}/k) \qquad (h \bmod k,\ ah\equiv b \pmod D))\\ &=(gD)^{-1}\sum_{l=0}^{k-1}c_l\sum_h{}'\omega(h,k)\exp(2\pi i\{-gDnh+gD(\nu\delta+l)\bar h\}/gDk) \qquad (h \bmod gDk,\ ah\equiv b \pmod D)).\end{aligned}$$

We define here an integer a' as any fixed solution of

$$(2.33)\qquad aa'\equiv 1 \pmod M.$$

Using (2.33), (2.31), (2.25) and the remark following (2.24), we get

$$(2.34)\qquad \begin{aligned}S_k=(gD)^{-1}\exp(2\pi iW)\sum_{l=0}^{k-1}c_l\sum_h{}'\exp(2\pi i\{(U-gDn)h\\ +(V\delta+gD(\nu\delta+l))\bar h\}/gDk)\\ (h \bmod gDk,\ h\equiv a'b \pmod D)).\end{aligned}$$

The inner sum, $T_k(l)$ say, is a generalized Kloosterman sum, and therefore admits of the estimate (see [1], [11], [13]):

$$|T_k(l)| < C_0(gDk)^{1-\alpha}(gDk, U - gDn)^{\beta}, \tag{2.35}$$

where α, β are any numbers satisfying $0 < \alpha < \beta < \frac{1}{2}$, and C_0 is a positive constant depending only on α and β.

Thus we obtain from (2.34), (2.35) and (2.29)

$$\begin{aligned} |S_k| &\leqq (gD)^{-1}\sum_{l=0}^{k-1}|c_l|\,|T_k(l)| \\ &< (gD)^{-1}C_0(gDk)^{1-\alpha}(gDk, U - gDn)^{\beta}\{1 + 2\sum_{l=1}^{\leqq k/2}(2l)^{-1}\} \\ &< C_0(gD)^{-\alpha}k^{1-\alpha}(gDk, U - gDn)^{\beta}\log(4k). \end{aligned} \tag{2.36}$$

On the other hand, by (2.24) and (2.21), we have

$$U = gD\gamma(aX + MY) - \phi\delta\{2K^2 + 3K(2a - M) + A\}.$$

But examination of (2.9) and (2.12) reveals that

$$gDX = kg(k_1 - 1)/2 \equiv 0 \pmod{k},$$

$$gDY = kg(k_1 - 1)(2k_1 - 1)/6 \equiv 0 \pmod{k}.$$

Hence

$$U \equiv -\phi\delta A \pmod{k}. \tag{2.37}$$

Using (2.37), (2.22), and recalling that $(f, k) = 1$, $fg = 12$, $(k_1, m_1) = 1$ and (1.1), we find

$$\begin{aligned} (gDk, U - gDn) &\leqq gD(k, U - gDn) = gD(k, -\phi\delta A - gDn) \\ &= gD(k, f\phi\delta A + fgDn) = gD(k, \delta A + 12Dn) \\ &\leqq gD^2(k_1, \delta A + 12Dn) = gD^2(k_1, \delta m_1 A + 12m_1 Dn) \\ &= gD^2(k_1, (\gamma k_1 - 1)A + 12Mn) = gD^2(k_1, 12Mn - A) \\ &\leqq gD^2\,|12Mn - A|, \end{aligned} \tag{2.38}$$

where the last inequality follows from the fact that

$$12Mn - A \neq 0 \quad \text{for } n = 0, 1, 2, \cdots. \tag{2.39}$$

To prove (2.39), suppose on the contrary that $12Mn - A = 0$ for some value of n. Then $A \equiv 0 \pmod{M}$, i.e. $A = 6a^2 - 6Ma + M^2 \equiv 0 \pmod{M}$, so that $6a^2 \equiv 0 \pmod{M}$. But we have assumed that $(a, M) = 1$, and so $6 \equiv 0 \pmod{M}$, which implies $M \leqq 6$. Moreover, since $0 < a < M$, we have $A < M^2$. Hence $n = A/12M < M/12 \leqq 6/12 = \frac{1}{2}$. Therefore $n = 0$, and we have $A = 0$, which implies that a/M is an irrational number, and this is clearly a contradiction.

By using (2.38), it follows from (2.36) that[3]

$$\begin{aligned}|S_k| &< C_0(gD)^{-\alpha}k^{1-\alpha}\{gD^2 \,|\, 12Mn - A\,|\}^{\beta}\log(4k) \\ &= C_0 g^{\beta-\alpha}D^{2\beta-\alpha}k^{1-\alpha}\,|\,12Mn - A\,|^{\beta}\log(4k) = O(k^{1-\alpha}(n+1)^{\beta}\log k) \\ &\hspace{20em}(n \geqq 0).\end{aligned}$$

Here we can omit the $\log k$ from the O-term since we may choose α arbitrarily large so far as $\alpha < \beta$.

Thus we conclude the following

THEOREM 2. *The sum S_k defined by* (2.26) *is subject to the estimate*

$$|S_k| < Ck^{1-\alpha}(n+1)^{\beta} \quad (n \geqq 0),$$

where α, β are any numbers satisfying $0 < \alpha < \beta < \frac{1}{2}$, and C is a constant depending only on α, β and M.

3. A convergent series for $p(n; a, M)$. We are now ready to apply the Hardy-Ramanujan method. We shall treat the partition function $p(n; a, M)$ for $n \geqq 0$, provided that $p(0; a, M) = 1$.

In the first place, we obtain, by Cauchy's theorem,[4]

$$p(n; a, M) = \frac{1}{2\pi i}\int_C x^{-n-1}F(x; a, M)\,dx.$$

Using the Farey dissection of order N, this becomes

$$\begin{aligned}p(n; a, M) &= \sum_{h,k}{}' \exp(-2\pi i n h/k) \\ (3.1) \qquad &\cdot \int_{-\theta'}^{\theta''} F(\exp(2\pi i h/k - 2\pi w); a, M)\exp(2\pi n w)\,d\phi \\ &(0 \leqq h < k \leqq N;\ \theta' = \theta'_{h,k},\ \theta'' = \theta''_{h,k};\ w = N^{-2} - i\phi).\end{aligned}$$

Now, in the transformation equation (1.8) we expand $F(x'; b, D, \rho)$ (see (1.4)) into a power series in x' as

$$\begin{aligned}F(x'; b, D, \rho) &= \prod_{m=0}^{\infty}(1 - \rho x'^{mD+b})^{-1}(1 - \rho^* x'^{mD+D-b})^{-1} \\ (3.2) \qquad &= \sum_{\nu=0}^{\infty} c_\nu(b, D, \rho)x'^{\nu},\end{aligned}$$

and substitute the relation (1.3), putting $z = kw$. Then (1.8) becomes

$$\begin{aligned}F(\exp(2\pi i h/k - 2\pi w); a, M) &= \omega(h, k)\exp\{(\pi/6Mk)(B/kw - Akw)\} \\ &\cdot \sum_{\nu=0}^{\infty} c_\nu(b, D, \rho)\exp(2\pi i \nu H/k - 2\pi\nu/Kkw).\end{aligned}$$

---

[3] We mean throughout the paper that the constant implied in the O-symbol always depends at most on α, β and M.

[4] For definitions of the unexplained notations in this section, see Rademacher [10].

Insertion of this into (3.1) yields

$$p(n;a,M)=\sum_{h,k}{}' \omega(h,k)\exp(-2\pi inh/k)\int_{-\theta'}^{\theta''}\sum_{\nu=0}^{\infty}c_\nu(b,D,\rho) \tag{3.3}$$
$$\cdot\exp\{(\pi/6Mk^2w)(B-12D\nu)-(\pi w/6M)(A-12Mn)\}\exp(2\pi i\nu H/k)d\phi.$$

We separate here the sum over ν into two parts as

$$\sum_{\nu=0}^{\infty}=\sum_{\nu=0}^{[B/12D]}+\sum_{\nu>[B/12D],\,\nu\geqq 0}$$

so that the coefficient of w^{-1} is always positive[5] in the first sum,[6] while it is negative in the second sum. The right member of (3.3) then splits into two parts according to the above separation. Let that one which corresponds to the first sum be $Q(n)$, and let the other be $R(n)$. Then it will be seen without difficulty, though we will not develop here the details, that, by using a method analogous to that of Rademacher [10] and applying the estimation in Theorem 2, one can obtain the following result:

$$p(n;a,M)=Q(n)+R(n),$$
$$Q(n)=2\pi\sum_{k=1}^{N}\sum_{\substack{0\leqq b<D\\(b,D)=1}}\sum_{\nu=0}^{[B/12D]}c_\nu(b,D,\rho)S_k\cdot L_k(n,\nu;B,D) \tag{3.4}$$
$$+O(N^{-\alpha}(n+1)^{\beta}\exp(2\pi nN^{-2})),$$
$$R(n)=O(N^{-\alpha}(n+1)^{\beta}\exp(2\pi nN^{-2})),$$

where

$$S_k=S_k(n,\nu;b,D;0,k)\quad (\text{see } (2.26)),$$

and[7]

$$L_k(n,\nu;B,D)$$
$$=\frac{1}{2\pi i}\int^{(0+)}\exp\{(\pi/6Mk^2w)(B-12D\nu)-(\pi w/6M)(A-12Mn)\}dw$$
$$=\begin{cases} k^{-1}(A-12Mn)^{-\frac12}(B-12D\nu)^{\frac12}J_1((\pi/3Mk)(A-12Mn)^{\frac12}(B-12D\nu)^{\frac12}) & \text{if } n<A/12M,\\ k^{-1}(12Mn-A)^{-\frac12}(B-12D\nu)^{\frac12}I_1((\pi/3Mk)(12Mn-A)^{\frac12}(B-12D\nu)^{\frac12}) & \text{if } n>A/12M,\end{cases} \tag{3.5}$$

$J_1(t)$, $I_1(t)$ being the Bessel functions of the first order.

[5] The fact that $B-12D\nu\neq 0$ for $\nu=0,1,2,\cdots$ may be verified in the same way as (2.39).

[6] If $B<0$, this sum becomes empty and is to be interpreted as zero.

[7] See Watson [12], p. 176, (1) and p. 181, (1). Notice that $J_1(z)=-J_{-1}(z)$ and $I_1(z)=I_{-1}(z)$.

In (3.4) we now divide the sum over k into two parts according as $D>1$ or $D=1$, noting that $D>1$ implies $b>0$, and that $D=1$ implies $b=0$, $B=1$. We then obtain from (3.4), by letting $N\to\infty$ for every fixed $n\geqq 0$,

$$\begin{aligned}(3.6)\qquad p(n;a,M) &= 2\pi\sum_k^{(1)}\sum_{\substack{1\leqq b<D\\(b,D)=1}}\sum_{\nu=0}^{[B/12D]} c_\nu(b,D,\rho)S_k\cdot L_k(n,\nu;B,D)\\ &\quad+2\pi\sum_k^{(2)} c_0(0,1,\rho)S_k'\cdot L_k(n,0;1,1)\\ &=p^{(1)}(n;a,M)+p^{(2)}(n;a,M),\end{aligned}$$

say,[8] where the sums $\sum^{(1)}{}_k$ and $\sum^{(2)}{}_k$ are taken over those k for which $D=(k,M)>1$ and $D=1$ respectively, and where

$$(3.7)\qquad S_k'=S_k(n,0;0,1;0,k).$$

Now let us consider $p^{(1)}(n;a,M)$ first. We see that $B/12D\geqq 0$ is equivalent to $|\frac{1}{2}D-b|\geqq 3^{\frac{1}{2}}D/6$, since

$$B=6b^2-6Db+D^2=6(\tfrac{1}{2}D-b)^2-\tfrac{1}{2}D^2$$

by (1.7). Therefore we can write

$$\begin{aligned}(3.8)\qquad p^{(1)}(n;a,M) &= 2\pi\sum_k^{(1)}\sum_{\substack{b=1\\(b,D)=1}}^{[\lambda D]}\sum_{\nu=0}^{[B/12D]}\{c_\nu(b,D,\rho)S_k(n,\nu;b,D;0,k)\\ &\quad+c_\nu(D-b,D,\rho)S_k(n,\nu;D-b,D;0,k)\}L_k(n,\nu;B,D)\end{aligned}$$

with the abbreviation $\lambda=(3-3^{\frac{1}{2}})/6$, where we have made use of the fact that B is unchanged when b is replaced by $D-b$. Further, from (3.2) we have, since $0\leqq\nu<B/12D<D/12<D$,

$$c_\nu(b,D,\rho)=\sum_{l,l'}\rho^l\rho^{*l'},$$

where the summation extends over all non-negative integers l, l' satisfying

$$(3.9)\qquad lb+l'(D-b)=\nu.$$

But, since $0\leqq\nu<\frac{1}{2}D$, $0<b<\frac{1}{2}D$, the only possible solution of (3.9) is $l'=0$, $l=\nu/b$ with $b\mid\nu$. Hence

$$(3.10)\qquad c_\nu(b,D,\rho)=\begin{cases}\rho^{\nu/b}, & \text{if } b\mid\nu,\\ 0, & \text{otherwise.}\end{cases}$$

Similarly

$$(3.11)\qquad c_\nu(D-b,D,\rho)=\begin{cases}\rho^{*\nu/b}, & \text{if } b\mid\nu,\\ 0, & \text{otherwise.}\end{cases}$$

---

[8] The series for $p^{(1)}(n;a,M)$ and $p^{(2)}(n;a,M)$ are in fact *absolutely* convergent, as may be seen from arguments in Section 4.

Hence, putting $\nu = br$, where $r = 0, 1, 2, \cdots, [B/12Db]$, we get from (3.8), (3.10) and (3.11)

$$(3.12)\qquad p^{(1)}(n; a, M) = 2\pi \sum_k{}^{(1)} \sum_{\substack{b=1\\(b,D)=1}}^{[\lambda D]} \sum_{r=0}^{[B/12Db]} A_k(n, r; b, D) L_k(n, br; B, D),$$

where

$$(3.13)\qquad A_k(n, r; b, D) = \sum_{\substack{h \bmod k\\ h \equiv \pm a'b(D)}} \rho^{\pm r} \omega(h, k) \exp\{2\pi i(-nh + brH)/k\}$$

by (2.26) and (2.33).

We remark further that the sum over b on the right of (3.12) is empty when $D = 2, 3, 4$. For, since $\lambda D = (3 - 3^{\frac{1}{2}})D/6 = 1.26 \cdots \times D/6$, we have $[\lambda D] = 0$ for $D = 2, 3, 4$, and $[\lambda D] \geqq 1$ for $D \geqq 5$.

We shall next discuss $p^{(2)}(n; a, M)$. By (2.26), the sum S_k' of (3.7) contains the root of unity $\omega(h, k)$ whose definition is, by (1.6),

$$(3.14)\qquad \omega(h, k) = \exp\{2\pi i \sigma(h, k)\}$$

with

$$(3.15)\qquad \sigma(h, k) = \sum_\mu (\mu/Mk - \tfrac{1}{2})(h\mu/k - [h\mu/k] - \tfrac{1}{2})$$
$$(\mu = a, M + a, 2M + a, \cdots, (k-1)M + a),$$

since $D = 1$ implies $K = Mk$, $k_1 = k$.

Now let ξ be an integer defined by

$$(3.16)\qquad \xi k \equiv a \pmod{M} \quad (0 < \xi < M),$$

which is uniquely solvable since $D = (k, M) = 1$. Let $\mu_0 = \xi k$. Then we see that $h\mu/k$ is integer if and only if $\mu = \mu_0$ because of $(h, k) = 1$, $\mu \equiv a \pmod{M}$ and $0 < \mu < Mk$.

Consequently we can write (3.15) in the form

$$(3.17)\qquad \begin{aligned}\sigma(h, k) &= \sum_{\mu \neq \mu_0} (\mu/Mk - \tfrac{1}{2})(h\mu/k - [h\mu/k] - \tfrac{1}{2}) + (\xi/M - \tfrac{1}{2})(-\tfrac{1}{2})\\ &= \tau(h, k) + \tfrac{1}{2}(\tfrac{1}{2} - \xi/M),\end{aligned}$$

where

$$(3.18)\qquad \tau(h, k) = \sum_\mu ((\mu/Mk))((h\mu/k))$$
$$(\mu = a, M + a, 2M + a, \cdots, (k-1)M + a)$$

with the notation

$$(3.19)\qquad ((t)) = \begin{cases} 0, & \text{if } t \text{ is an integer,}\\ t - [t] - \tfrac{1}{2}, & \text{otherwise.}\end{cases}$$

It therefore follows from (3.14) and (3.17) that

$$(3.20)\qquad \omega(h, k) = i \exp(-\pi i \xi/M) \chi(h, k)$$

with

$$(3.21)\qquad \chi(h,k)=\exp\{2\pi i\tau(h,k)\}$$

On the other hand, (1.1) becomes

$$(3.22)\qquad \gamma k-\delta M=1,$$

since $D=1$ implies $k_1=k$, $m_1=M$. From (3.16) and (3.22) it follows that $\gamma a\equiv\xi\pmod M$, and hence, by the definition of ρ in (1.5), we have $\rho=\exp(-2\pi i\xi/M)$, so that

$$(3.23)\qquad (1-\rho)^{-1}=(2i)^{-1}\csc(\pi\xi/M)\exp(\pi i\xi/M).$$

Further, it is evident from (3.2) that

$$(3.24)\qquad c_0(0,1,\rho)=(1-\rho)^{-1}.$$

Thus we infer from (3.24), (3.23), (3.7), (2.26) and (3.20) that

$$(3.25)\qquad c_0(0,1,\rho)S_k'=\tfrac{1}{2}\csc(\pi\xi/M)B_k(n),$$

where

$$(3.26)\qquad B_k(n)=\sum_{h \bmod k}{}' \chi(h,k)\exp(-2\pi inh/k)$$

with the $\chi(h,k)$ of (3.21). From (3.6) and (3.25) we obtain the expression:

$$(3.27)\qquad p^{(2)}(n;a,M)=\pi\sum_k{}^{(2)}\csc(\pi\xi/M)B_k(n)L_k(n,0;1,1).$$

Finally, we define an integer k' as any fixed solution of

$$(3.28)\qquad kk'\equiv 1 \pmod M,$$

which, combined with (3.16), yields that $\xi\equiv ak'\pmod M$. Hence

$$(3.29)\qquad \csc(\pi\xi/M)=|\csc(\pi ak'/M)|.$$

We note, in addition, that when $D>1$ we can express $\sigma(h,k)$ in a form corresponding to (3.18), namely,

$$(3.30)\qquad \sigma(h,k)=\sum_\mu((\mu/K))((h\mu/k))$$
$$(\mu=a, M+a, 2M+a,\cdots,(k_1-1)M+a).$$

For we see that $0<\mu/K<1$ and that $D>1$ implies $h\mu/k\neq$ integer since the congruence $\xi k\equiv a\pmod M$ has no solution in ξ as we have assumed that $(a,M)=1$, and the result follows from (1.6) and (3.19).

On combining (3.6), (3.12), (3.27), (3.29) and the remark following (3.13) we obtain our main result (cf. [6], Theorem 4):

THEOREM 3. *If $p(n;a,M)$ denotes, when $n \geqq 1$, the number of partitions of n into positive summands congruent to $\pm a \pmod{M}$, and $p(0;a,M) = 1$, where $M \geqq 3$, $0 < a < M$, $(a,M) = 1$, then we have, for $n \geqq 0$, the convergent series representation*

$$p(n;a,M) = 2\pi \sum_{\substack{k>0 \\ D\geqq 5}} \sum_{\substack{b=1 \\ (b,D)=1}}^{[\lambda D]} \sum_{r=0}^{[B/12Db]} A_k(n,r;b,D) L_k(n,br;B,D) + \pi \sum_{\substack{k>0 \\ D=1}} |\csc(\pi ak'/M)| B_k(n) L_k(n,0;1,1),$$

where $A_k(n,r;b,D)$ and $B_k(n)$ are given by (3.13) and (3.26) with $\omega(h,k)$ and $\chi(h,k)$ defined by (1.6), (3.30) and (3.21), (3.18) respectively; $L_k(n,br;B,D)$ and $L_k(n,0;1,1)$ by (3.5); k' by (3.28); and $\lambda = (3 - 3^{\frac{1}{2}})/6$.

Remark. The sums A_k, B_k defined by (3.13), (3.26) have the following properties:

(i) A_k, B_k are always *real.*

(ii) The value of A_k is *independent* of the choice of γ, δ in (1.1).

(i) may easily be verified, e.g. for A_k, if in (3.13) one divides the sum into two parts according as $h \equiv + a'b \pmod{D}$ or $h \equiv - a'b \pmod{D}$, observing that the divided two sums are conjugate complex numbers because the $\sigma(h,k)$ of (3.30) and the H of (1.2) are both odd functions in the variable h (H is to be considered modulo k). Similarly for B_k.

Referring to (ii) we note that, although the formula (3.13) involves ρ and H which, by (1.5) and (1.2), depend upon the choice of γ, δ, the value of A_k remains unaffected by ρ, H. This follows from the fact that in (3.13) $\rho^{\pm r}\exp(2\pi ibrH/k)$ are actually independent of ρ and H. To show this, we make use of (1.15). Now let that value of μ for which $\mu^* = b$ be μ_b. Then (1.15) gives

$$\mu_b/K \equiv -Hb/k + \gamma a/M \pmod{1},$$

so that

$$\exp(-2\pi i\mu_b/K) = \rho \exp(2\pi ibH/k) \tag{3.31}$$

by the definition of ρ in (1.5). Next, let that value of μ for which $\mu^* = (k_1 - 1)D + b = k - (D - b)$ be $\mu_{k-(D-b)}$. Then, by (1.15),

$$\mu_{k-(D-b)}/K \equiv H(D - b - k)/k + \gamma a/M \pmod{1},$$

so that

$$\exp(2\pi i\mu_{k-(D-b)}/K) = \rho^{-1}\exp(2\pi i(D - b)H/k),$$

or, replacing $D-b$ by b,

$$\exp(2\pi i\mu_{k-b}/K)=\rho^{-1}\exp(2\pi ibH/k). \tag{3.32}$$

The desired result then follows from (3.31) and (3.32) on taking the r-th powers.

4. Asymptotic properties of $p(n; a, M)$. We require first a lemma on $I_1(t)$, the Bessel function of the first order with purely imaginary argument.

LEMMA 4.1.

(4.1) *$I_1(t)$ is positive and increasing for $t>0$.*

(4.2) $I_1(t)=O(t) \quad (t\to 0)$.

(4.3) $I_1(t)=(2\pi t)^{-\frac{1}{2}}e^t(1+O(t^{-1})) \quad (t\to+\infty)$.

Proof. (4.1) and (4.2) are easy consequences of the expansion:

$$I_1(t)=\sum_{m=0}^{\infty}(\tfrac{1}{2}t)^{2m+1}/m!(m+1)!$$

(see Watson [12], p. 77, (2));

and (4.3) is obtained from [12], p. 203.

The following lemma will be also needed.

LEMMA 4.2. *Let*

$$S_1(N)=\sum_{\nu=1}^{N}\nu^{\frac{1}{2}}e^{N/\nu}, \qquad S_2(N)=\sum_{\nu=2}^{N}\nu^{\frac{1}{2}}e^{N/\nu}.$$

Then $S_1(N)<2e^N$ for $N\geqq 6$, and $S_2(N)<5e^{\frac{1}{2}N}$ for $N\geqq 12$.

Proof. Since $t^{\frac{1}{2}}e^{N/t}$ is decreasing for $1\leqq t\leqq N$, we have

$$S_1(N)\leqq e^N+\int_1^N t^{\frac{1}{2}}e^{N/t}\,dt=e^N+N^{\frac{3}{2}}\int_1^N y^{-\frac{5}{2}}e^y\,dy \quad (N/t=y). \tag{4.4}$$

Here, since $y^{-\frac{5}{2}}e^y$ is decreasing for $1\leqq y\leqq\frac{5}{2}$ and increasing for $y\geqq\frac{5}{2}$, it follows that

$$y^{-\frac{5}{2}}e^y\leqq\max(e, N^{-\frac{5}{2}}e^N) \quad (1\leqq y\leqq N). \tag{4.5}$$

But we have $-\frac{5}{2}\log 6+6=1.5\cdots>1$, so that $N^{-\frac{5}{2}}e^N>e$ for $N\geqq 6$. Hence, by (4.5),

$$y^{-\frac{5}{2}}e^y\leqq N^{-\frac{5}{2}}e^N \quad (1\leqq y\leqq N, N\geqq 6).$$

Therefore

$$\int_1^N y^{-\frac{5}{2}} e^y \, dy < N \cdot N^{-\frac{5}{2}} e^N = N^{-\frac{3}{2}} e^N \quad (N \geqq 6),$$

which, together with (4.4), yields the first inequality in our lemma. The second may be proved similarly.

We now determine the asymptotic behavior of $p(n; a, M)$ as n becomes large. By Theorem 3, we have

$$(4.6) \qquad p(n; a, M) = p^{(1)}(n; a, M) + p^{(2)}(n; a, M),$$

where

$$(4.7) \qquad p^{(1)}(n; a, M) = 2\pi \sum_k^{(1)} \sum_{\substack{b=1 \\ (b,D)=1}}^{[\lambda D]} \sum_{r=0}^{[B/12Db]} A_k(n, r; b, D) L_k(n, br; B, D),$$

$$(4.8) \qquad p^{(2)}(n; a, M) = \pi \sum_k^{(2)} |\csc(\pi a k'/M)| B_k(n) L_k(n, 0; 1, 1),$$

$$\Big(\sum_k^{(1)} = \sum_{k>0,\, D\geqq 5}, \ \sum_k^{(2)} = \sum_{k>0,\, D=1} \Big)$$

in which

$$(4.9) \quad L_k(n, br; B, D) = (kE)^{-1}(B - 12Dbr)^{\frac{1}{2}} I_1((\pi E/3Mk)(B - 12Dbr)^{\frac{1}{2}})$$

$$(4.10) \quad L_k(n, 0; 1, 1) = (kE)^{-1} I_1(\pi E/3Mk)$$

with the abbreviation

$$(4.11) \qquad E = (12Mn - A)^{\frac{1}{2}} \quad (n > A/12M).$$

Let us begin with $p^{(1)}(n; a, M)$. Clearly it suffices to consider the case $M \geqq 5$. Now if we keep D fixed, B takes its maximum value when $b = 1$, i.e., the value $B_1 = 6 - 6D + D^2$, since

$$B = 6b^2 - 6Db + D^2 = 6(\tfrac{1}{2}D - b)^2 - \tfrac{1}{2}D^2$$

and $1 \leqq b < \frac{1}{2}D$. Hence from (4.9) and (4.1) we get

$$(4.12) \qquad L_k(n, br; B, D) \leqq (kE)^{-1}(B - 12Dbr)^{\frac{1}{2}} I_1(\pi E B_1^{\frac{1}{2}}/3Mk).$$

On the other hand, from (3.13) we have trivially

$$(4.13) \qquad |A_k(n, r; b, D)| \leqq \sum_{\substack{h \bmod k \\ h \equiv \pm a'b(D)}}' 1 < k,$$

while, by Theorem 2, we have the non-trivial estimate [9]

$$(4.14) \qquad |A_k(n, r; b, D)| < C_1 k^{1-\alpha}(n+1)^\beta \quad (0 < \alpha < \beta < \tfrac{1}{2}).$$

[9] In what follows we shall use $C_1, C_2, \cdots, C_{10}$ to denote certain positive constants depending at most on α, β and M.

From (4.12), (4.13) and (4.14) it follows that

$$(4.15)\qquad \Big|\sum_{\substack{b=1\\(b,D)=1}}^{[\lambda D]}\sum_{r=0}^{[B/12Db]} A_k(n,r;b,D)L_k(n,br;B,D)\Big| < \begin{cases} E^{-1}Z_D I_1(\pi E B_1^{\frac{1}{2}}/3Mk),\\ C_1E^{-1}k^{-\alpha}(n+1)^{\beta}Z_D I_1(\pi EB_1^{\frac{1}{2}}/3Mk)\end{cases}$$

with the abbreviation

$$Z_D=\sum_{\substack{b=1\\(b,D)=1}}^{[\lambda D]}\sum_{r=0}^{[B/12Db]}(B-12Dbr)^{\frac{1}{2}}.$$

Using (4.15) and noting that

$$\sum_k{}^{(1)}=\sum_{\substack{D\mid M\\D\geqq 5}}\sum_{\substack{k_1=1\\(k_1,m_1)=1}}^{\infty},$$

where $k=k_1D$, $M=m_1D$, we get, by (4.7),

$$(4.16)\qquad \begin{aligned}|p^{(1)}(n;a,M)| &< 2\pi\sum_{\substack{D\mid M\\D\geqq 5}}\sum_{k_1=1}^{\leqq F}E^{-1}Z_DI_1(F/k_1)\\ &\quad+2\pi\sum_{\substack{D\mid M\\D\geqq 5}}\sum_{k_1>F}C_1E^{-1}D^{-\alpha}k_1^{-\alpha}(n+1)^{\beta}Z_DI_1(F/k_1),\end{aligned}$$

where

$$(4.17)\qquad F=\pi EB_1^{\frac{1}{2}}/3MD.$$

But it follows from (4.2), (4.3) and Lemma 4.2 that

$$(4.18)\qquad \begin{aligned}\sum_{k_1=1}^{\leqq F}I_1(F/k_1) &< C_2\sum_{k_1=1}^{\leqq F}(2\pi F/k_1)^{-\frac{1}{2}}e^{F/k_1}\\ &=C_2(2\pi F)^{-\frac{1}{2}}\sum_{k_1=1}^{\leqq F}k_1^{\frac{1}{2}}e^{F/k_1}<C_3F^{-\frac{1}{2}}e^F,\\ \sum_{k_1>F}k_1^{-\alpha}I_1(F/k_1) &< C_4F\sum_{k_1>F}k_1^{-1-\alpha}<C_5F^{1-\alpha}.\end{aligned}$$

Now, set

$$(4.19)\qquad G=\pi E/3M.$$

Then we have

$$(4.20)\qquad F=GB_1^{\frac{1}{2}}/D$$

by (4.17). Further, since $5\leqq D\leqq M$ and

$$B_1/D^2=1-6/D+6/D^2=6(\tfrac{1}{2}-1/D)^2-\tfrac{1}{2},$$

we have

$$6(\tfrac{1}{2}-\tfrac{1}{5})^2-\tfrac{1}{2}\leqq B_1/D^2\leqq 6(\tfrac{1}{2}-1/M)^2-\tfrac{1}{2},$$

i.e.,

$$\tfrac{1}{25} \leqq B_1/D^2 \leqq M_1^2,$$

where

$$M_1 = (1 - 6/M + 6/M^2)^{\frac{1}{2}} < 1. \tag{4.21}$$

Thus we obtain $\frac{1}{5} \leqq B_1^{\frac{1}{2}}/D \leqq M_1 < 1$, and hence, noting (4.20),

$$G/5 \leqq F \leqq M_1 G < G. \tag{4.22}$$

From (4.16), (4.18) and (4.22) we deduce

$$\begin{aligned} | p^{(1)}(n; a, M) | &< 2\pi C_3 E^{-1} (G/5)^{-\frac{3}{2}} e^{M_1 G} \sum_{\substack{D \mid M \\ D \geqq 5}} Z_D \\ &\quad + 2\pi C_1 C_5 E^{-1} G^{1-\alpha} (n+1)^{\beta} \sum_{\substack{D \mid M \\ D \geqq 5}} D^{-\alpha} Z_D \\ &= C_6 E^{-1} G^{-\frac{3}{2}} e^{M_1 G} + C_7 E^{-1} G^{1-\alpha} (n+1)^{\beta}. \end{aligned} \tag{4.23}$$

We next treat $p^{(2)}(n; a, M)$. In (4.8) we distinguish the term $k=1$ from the others, and obtain

$$\begin{aligned} p^{(2)}(n; a, M) &= \pi \csc(\pi a/M) B_1(n) L_1(n, 0; 1, 1) \\ &\quad + \pi \sum_{k>1}{}^{(2)} | \csc(\pi a k'/M) | B_k(n) L_k(n, 0; 1, 1). \end{aligned} \tag{4.24}$$

Here evidently

$$| \csc(\pi a k'/M) | \leqq \csc(\pi/M) < \tfrac{1}{2}\pi (M/\pi) = \tfrac{1}{2} M. \tag{4.25}$$

Further we get

$$| B_k(n) | < k, \tag{4.26}$$

$$| B_k(n) | < C_8 k^{1-\alpha} (n+1)^{\beta} \qquad (0 < \alpha < \beta < \tfrac{1}{2}), \tag{4.27}$$

which correspond to (4.13), (4.14).

From (4.10), (4.19), (4.25), (4.26), (4.27) we obtain

$$\begin{aligned} &\Big| \pi \sum_{k>1}{}^{(2)} | \csc(\pi a k'/M) | \, B_k(n) L_k(n, 0; 1, 1) \Big| \\ &\quad < \pi \sum_{k=2}^{\leqq G} \tfrac{1}{2} M k (kE)^{-1} I_1(G/k) \\ &\qquad + \pi \sum_{k>G} \tfrac{1}{2} M C_8 k^{1-\alpha} (n+1)^{\beta} I_1(G/k) \\ &\quad < C_9 E^{-1} G^{-\frac{3}{2}} e^{\frac{1}{2}G} + C_{10} E^{-1} G^{1-\alpha} (n+1)^{\beta}, \end{aligned} \tag{4.28}$$

where in the last step we have made use of (4.2), (4.3) and Lemma 4.2.

On the other hand, we have

$$B_1(n) = 1 \tag{4.29}$$

by (3.26), and

$$L_1(n,0;1,1)=E^{-1}I_1(G)=E^{-1}(2\pi G)^{-\frac{1}{2}}e^G(1+O(G^{-1})) \tag{4.30}$$

by (4.3).

It now follows from (4.6), (4.23), (4.24), (4.28), (4.29) and (4.30) that

$$p(n;a,M)=\pi\csc(\pi a/M)E^{-1}I_1(G)$$
$$\cdot\{1+O(e^{M_1G-G})+O(e^{-\frac{1}{2}G})+O(G^{\frac{3}{2}-\alpha}(n+1)^{\beta}e^{-G})\}$$

Substituting from (4.11), (4.19), we are led to the following

THEOREM 4. *We have*

$$p(n;a,M)=\pi\csc(\pi a/M)\cdot(12Mn-A)^{-\frac{1}{2}}$$
$$\cdot I_1((\pi/3M)(12Mn-A)^{\frac{1}{2}})\{1+O(\exp(-cn^{\frac{1}{2}}))\},$$

where c is a positive constant defined by

$$c=2\pi(3M)^{-\frac{1}{2}}\min(\tfrac{1}{2},1-M_1)$$

with the M_1 of (4.21).

From Theorem 4 and (4.3), we can easily find an asymptotic formula for $p(n;a,M)$ in terms of elementary functions of n. We have

$$p(n;a,M)=\csc(\pi a/M)\cdot(3M/2)^{\frac{1}{4}}(12Mn-A)^{-\frac{3}{4}}$$
$$\cdot\exp((\pi/3M)(12Mn-A)^{\frac{1}{2}})\{1+O(n^{-\frac{1}{2}})\},$$

or further

$$p(n;a,M)=\tfrac{1}{4}\csc(\pi a/M)\cdot(3M)^{-\frac{1}{4}}n^{-\frac{3}{4}}\exp(2\pi(n/3M)^{\frac{1}{2}})\{1+O(n^{-\frac{1}{2}})\}. \tag{4.31}$$

This formula will also be deduced, apart from the error term, from a result of Meinardus [7].

Finally, it is readily seen from (4.31) that, for any two values a_1, a_2 of a, we have

$$\lim_{n\to\infty}(p(n;a_1,M):p(n;a_2,M))=\csc(\pi a_1/M):\csc(\pi a_2/M).$$

DEFENSE ACADEMY, YOKOSUKA, JAPAN.

REFERENCES.

[1] T. Estermann, "Vereinfachter Beweis eines Satzes von Kloosterman," *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität*, vol. 7 (1929), pp. 82-98.

[2] L. K. Hua, "On the number of partitions of a number into unequal parts," *Transactions of the American Mathematical Society*, vol. 51 (1942), pp. 194-201.

[3] S. Iseki, "The transformation formula for the Dedekind modular function and related functional equations," *Duke Mathematical Journal*, vol. 24 (1957), pp. 653-662.

[4] ———, "Some transformation equations in the theory of partitions," *Proceedings of the Japan Academy*, vol. 34 (1958), pp. 131-135.

[5] J. Lehner, "A partition function connected with the modulus five," *Duke Mathematical Journal*, vol. 8 (1941), pp. 631-655.

[6] J. Livingood, "A partition function with the prime modulus $p > 3$," *American Journal of Mathematics*, vol. 67 (1945), pp. 194-208.

[7] G. Meinardus, "Asymptotische Aussagen über Partitionen," *Mathematische Zeitschrift*, vol. 59 (1954), pp. 388-398.

[8] I. Niven, "On a certain partition function," *American Journal of Mathematics*, vol. 62 (1940), pp. 353-364.

[9] H. Rademacher, "On the partition function $p(n)$," *Proceedings of the London Mathematical Society*, (2), vol. 43 (1937), pp. 241-254.

[10] ———, "The Fourier coefficients of the modular invariant $J(\tau)$," *American Journal of Mathematics*, vol. 60 (1938), pp. 501-512.

[11] H. Salié, "Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen," *Mathematische Zeitschrift*, vol. 36 (1933), pp. 263-278.

[12] G. N. Watson, *A treatise on the theory of Bessel functions*, Cambridge, 1944.

[13] A. Weil, "On some exponential sums," *Proceedings of the National Academy of Sciences, U. S. A.*, vol. 34 (1948), pp. 204-207.

DIFFERENTIABLE STRUCTURES ON SPHERES.*

By JOHN MILNOR.[1]

According to [5] the sphere S^7 can be given several differentiable structures which are essentially distinct. A corresponding result for the 15-sphere has been proved by Shimada [10] and Tamura [12]. The object of this note is to prove corresponding theorems for other dimensions of the form $4k-1$.

In § 1 certain differentiable manifolds $M(f_1, f_2)$ are constructed and studied; where $(f_1) \in \pi_m(SO_{n+1})$, $(f_2) \in \pi_n(SO_{m+1})$. In most cases these manifolds are topologically spheres. In § 2 an invariant λ is defined for differentiable $(4k-1)$-manifolds which are both homology spheres and boundaries. In § 3 the invariant $\lambda(M(f_1, f_2))$ is computed.

For $k \leqq 8$ the calculations are carried out explicitly. It is shown that there exist non-standard differentiable structures on S^{4k-1} for $k = 2, 4, 5, 6, 7, 8$. For example S^{31} has over sixteen million distinct differentiable structures. It is conjectured that the same argument works for all $k \geqq 4$; but I have not succeeded in solving the number theoretic problem which arises.

For $k = 1, 3$ the argument does not work. This is not surprising in the case $k = 1$, since J. Munkres, S. Smale, and J. H. C. Whitehead have shown (independently) that two differentiable 3-manifolds which are homeomorphic must necessarily be diffeomorphic.

The word *manifold* will always be used for a compact, oriented manifold, with or without boundary. The symbol D^k will stand for the unit disk in the euclidean space R^k.

1. Construction of manifolds homeomorphic to spheres. Given any diffeomorphism[2] $f\colon S^m \times S^n \to S^m \times S^n$, a manifold M of dimension $m+n+1$ is obtained by matching the boundaries of $D^{m+1} \times S^n$ and $S^m \times D^{n+1}$ under the correspondence f. That is: M is the identification space obtained from the disjoint union of $D^{m+1} \times S^n$ and $S^m \times D^{n+1}$ by identifying each point (x, y) in the boundary of $D^{m+1} \times S^n$ with $f(x, y)$, considered as a point in boundary of $S^m \times D^{n+1}$.

* Received February 10, 1959.

[1] The author holds a Sloan fellowship.

[2] A *diffeomorphism* is a differentiable homeomorphism with differentiable inverse.

An alternative definition of M, which makes it into a differentiable manifold, is the following. Let $f(x,y)=(x',y')$ and define $t'=1/t$. Start with disjoint spaces $R^{m+1}\times S^n$ and $S^m\times R^{n+1}$. Let M be obtained from these by matching (tx,y) with $(x',t'y')$ for every $x\in S^m$, $y\in S^n$, $0<t<\infty$.

[As an example suppose that f is the identity map of $S^m\times S^n$. Then M is diffeomorphic to the unit sphere $S^{m+n+1}\subset R^{m+1}\times R^{n+1}$. In fact the correspondence

$$(tx,y)\to(tx/(1+t^2)^{\frac{1}{2}},y/(1+t^2)^{\frac{1}{2}}),$$
$$(x',t'y')\to(x'/(1+t'^2)^{\frac{1}{2}},t'y'/(1+t'^2)^{\frac{1}{2}})$$

defines a diffeomorphism $M\to S^{m+n+1}$.]

If $y\in S^n$ has coordinates $(y_0,\cdots,y_n)$, define $h(y)=y_n$. The function $h\colon S^n\to[-1,1]$ has just two critical points.

LEMMA 1. *Suppose that the diffeomorphism*

$$(x,y)\xrightarrow{f}(x',y')$$

satisfies the restriction $h(y)=h(y')$ for all (x,y). Then the manifold M constructed above is homeomorphic to S^{m+n+1}.

Proof. A differentiable map $g\colon M\to[-1,1]$ is defined by the correspondence

$$(tx,y)\to h(y)/(1+t^2)^{\frac{1}{2}} \text{ (in the first coordinate system)},$$
$$(x',t'y')\to t'h(y')/(1+t'^2)^{\frac{1}{2}} \text{ (in the second)}.$$

It is easily verified that g has just two critical points, and that these are non-degenerate. Together with [5] Theorem 2, this completes the proof.

One way to construct such a diffeomorphism $(x,y)\to(x',y')$ is the following. Start with differentiable maps of spheres into rotation groups

$$f_1\colon S^m\to SO_{n+1},\qquad f_2\colon S^n\to SO_{m+1},$$

and let

$$y'=f_1(x)\cdot y,\qquad x'=f_2(y')^{-1}\cdot x=f_2(f_1(x)\cdot y)^{-1}\cdot x$$

for all $x\in S^m$, $y\in S^n$. This defines a diffeomorphism with inverse

$$x=f_2(y')\cdot x',\qquad y=f_1(x)^{-1}\cdot y'=f_1(f_2(y')\cdot x')^{-1}\cdot y'.$$

[More generally the rotation groups SO_{n+1} and SO_{m+1} could be replaced by the groups Diff S^n, Diff S^m consisting of all diffeomorphisms.] The condition $h(y)=h(y')$ is equivalent to the requirement that $f_1(S^m)$ be contained in

the subgroup $SO_n \subset SO_{n+1}$. Whether this condition is satisfied or not, *the resulting* $(m+n+1)$*-manifold will be denoted by* $M(f_1, f_2)$.

Next we will show that $M(f_1, f_2)$ is a boundary. Start with three copies of the space $D^{m+1} \times D^{n+1}$. The notation (x_i, y_i) will be used for a point of $(D^{m+1} \times D^{n+1})_i$, $i = 1, 2, 3$. Identify $(S^m \times D^{n+1})_1$ with $(S^m \times D^{n+1})_2$ by the correspondence $(x_1, y_1) \to (x_2, y_2)$ where

$$x_2 = x_1, \qquad y_2 = f_1(x_1) \cdot y_1.$$

The resulting space $(D^{m+1} \times D^{n+1})_1 \cup (D^{m+1} \times D^{n+1})_2$ can be considered as a fibre bundle over the $(m+1)$-sphere $(D^{m+1})_1 \cup (D^{m+1})_2$ with fibre D^{n+1}, group SO_{n+1}, and characteristic map f_1. (See Steenrod [11] § 18.) It follows that this union can be given a differentiable structure in a natural way.

Next identify $(D^{m+1} \times S^n)_2$ with $(D^{m+1} \times S^n)_3$ by the correspondence $(x_2, y_2) \leftarrow (x_3, y_3)$, where $y_2 = y_3$, $x_2 = f_2(y_3) \cdot x_3$. Thus

$$(D^{m+1} \times D^{n+1})_2 \cup (D^{m+1} \times D^{n+1})_3$$

becomes a fibre bundle over an $(n+1)$-sphere with fibre D^{m+1} and characteristic map f_2.

Let W_1 denote the union of all three copies of $D^{m+1} \times D^{n+1}$. Clearly W_1 is a topological manifold with boundary:

$$\partial W_1 = (D^{m+1} \times S^n)_1 \cup (S^m \times D^{n+1})_3.$$

The intersection

$$(D^{m+1} \times S^n)_1 \cap (S^m \times D^{n+1})_3$$

of the two halves of the boundary is equal to $(S^m \times S^n)_1 = (S^m \times S^n)_3$. These two copies of $S^m \times S^n$ are identified under the composite correspondence

$$(x_1, y_1) \to (x_2, y_2) \to (x_3, y_3),$$

where

$$y_3 = y_2 = f_1(x_1) \cdot y_1, \qquad x_3 = f_2(y_3)^{-1} \cdot x_2 = f_2(y_3)^{-1} \cdot x_1.$$

But this is just the correspondence which was used to define the manifold $M(f_1, f_2)$. Thus ∂W_1 is homeomorphic to $M(f_1, f_2)$.

As it stands W_1 is not a differentiable manifold since there is an "angle" along the subset $(S^m \times S^n)_1$ of ∂W_1. Let W denote a differentiable manifold obtained by "straightening" this angle. (See the appendix to [7].) Clearly ∂W is diffeomorphic to $M(f_1, f_2)$.

2. The invariant $\lambda(M)$. First recall the index theorem of Hirzebruch [4]. If M_1 is a $4k$-manifold without boundary having Pontrjagin classes

$p_1,\cdots,p_k$, then the index $I(M_1)$ is equal to $L_k(p_1,\cdots,p_k)[M_1]$; where L_k is a certain polynomial.[3] For example

$$L_1 = p_1/3, \qquad L_2 = (7p_2 - p_1{}^2)/45, \cdots.$$

The coefficient s_k of p_k in L_k is particularly important. Hirzebruch expresses s_k in terms of the Bernoulli number B_k as follows (page 14):

$$s_k = 2^{2k}(2^{2k-1} - 1)B_k/(2k)!.$$

For example $s_2 = 7/45$, $s_3 = 62/945$, $s_4 = 127/4725$.

Now let M be a differentiable $(4k-1)$-manifold which

1) has the same rational homology groups as the $(4k-1)$-sphere,

and

2) is a boundary: $M = \partial W$ with W differentiable.[4] Then a rational number modulo 1,

$$\lambda(M) \in Q/Z,$$

is defined as follows. The natural homomorphism

$$j\colon H^i(W,M;Q) \to H^i(W;Q)$$

is an isomorphism for $0 < i < 4k-1$. Hence the Pontrjagin classes $p_1,\cdots,p_{k-1}$ of W can be lifted back to $H^*(W,M;Q)$. Define $\lambda(M)$ as the residue class of

$$(I(W) - L_k(j^{-1}p_1,\cdots,j^{-1}p_{k-1},0)[W])/s_k$$

modulo 1. (Here the symbol $[W]$ stands for the homomorphism $H^{4k}(W,M;Q) \to Q$ associated with the orientation of W; and $I(W)$ denotes the index of the quadratic form $\alpha \to (\alpha \cup \alpha)[W]$, where $\alpha \in H^{2k}(W,M;Q)$.)

LEMMA 2. *This residue class $\lambda(M)$ is an invariant of M: that is it does not depend on the choice of W.*

The proof is completely analogous to that in [5], [10] or [12]. If M is the boundary of both W_1 and W_2, then an unbounded $4k$-manifold M_1 is obtained from W_1, W_2 by

---

[3] The symbol $[M_1]$ is used to denote the homomorphism of $H^{4k}(M_1;Q)$ into the rational numbers Q which is determined by an orientation for M_1. The index $I(M_1)$ is defined as the index of the quadratic form over $H^{2k}(M_1;Q)$ which is given by the formula $\alpha \to (\alpha \cup \alpha)[M_1]$.

[4] This second condition follows automatically if $H_*(M;Z)$ has no torsion. In fact every homology $(4k-1)$-sphere is a π-manifold (see [7]), and every π-manifold is a boundary (see [8]).

1) reversing the orientation of W_2;

2) matching W_1 and W_2 along the common boundary M;

3) constructing a differentiable structure in a neighborhood of $W_1 \cap W_2 = M$. (See [6] Lemma 4 or [7]). Then $I(M_1) = I(W_1) - (W_2)$; and each Pontrjagin number $p_{i_1} \cdots p_{i_r}[M_1]$ other than $p_k[M_1]$ is equal to the difference of corresponding Pontrjagin numbers for W_1, W_2. Now the index theorem for M_1 implies that the two definitions of $\lambda(M)$ differ only by the integer $p_k[M_1]$.

Example 1. For the $(4k-1)$-sphere it is clear that

$$\lambda(S^{4k-1}) \equiv 0 \pmod 1.$$

Example 2. For a 3-manifold the definition reduces to

$$\lambda(M^3) \equiv 3 \cdot I(W) \equiv 0 \pmod 1.$$

Example 3. For the 7-manifold $M_3{}^7$ of [5] the values

$$I(W) = 1, \quad (j^{-1}p_1)^2[W] = 36$$

give

$$\lambda(M_3{}^7) \equiv (45 I(W) + (j^{-1}p_1)^2[W])/7 \equiv 4/7 \pmod 1.$$

Remark. If $H^*(M;Z)$ has no torsion, then the classes $j^{-1}p_i$ can be considered as integral cohomolgy classes, hence the Pontrjagin numbers of W are integers. This sharply restricts the denominator which $\lambda(M)$ can have. (For example $7\lambda(M^7)$ must be an integer.) On the other hand, if $H^*(M;Z)$ has torsion then arbitrarily large denominators may occur. (See the examples studied by Tamura.)

Example 4. In [7] § 4 certain homotopy spheres $M_0{}^{4k-1}$ are constructed for $k > 1$. These have the property that $M_0{}^{4k-1} = \partial W$, where W is parallelizable, and $I(W) = 8$. Thus

$$\lambda(M_0{}^{4k-1}) \equiv 8/s_k \pmod 1.$$

For $k = 2$ this gives $\lambda(M_0{}^7) \equiv 3/7$ with denominator 7. For $k = 3, 4, 5, 6, 7$ the denominator of $\lambda(M_0{}^{4k-1})$ is 31, 127, 73, 1414477, and 8191 respectively. (These numbers are prime, except for $1414477 = 23 \cdot 89 \cdot 691$.) I do not know whether the inequality $8/s_k \not\equiv 0 \pmod 1$ holds for all $k > 1$.

In conclusion, the following three properties of the invariant λ are easily verified.

1) If the orientation of M is reversed, then λ changes sign.

2) For the connected sum of manifolds (see [7]), λ satisfies

$$\lambda(M_1 \# M_2) \equiv \lambda(M_1) + \lambda(M_2) \pmod 1.$$

3) λ is an invariant of the J-equivalence class of M. (See Thom [13] or [7].)

3. Computation of $\lambda(M(f_1, f_2))$. Define the *Pontrjagin homomorphism*

$$p_r: \pi_{4r-1}(SO_q) \to Z$$

as follows. Every map $f: S^{4r-1} \to SO_q$ induces a bundle ξ over S^{4r} with Pontrjagin class $p_r(\xi) \in H^{4r}(S^{4r}; Z) \approx Z$. Define $p_r(f)$ as the corresponding integer $p_r(\xi)[S^{4r}]$.

Let $f_1: S^m \to SO_{n+1}$, $f_2: S^n \to SO_{m+1}$ be arbitrary differentiable maps, with $m + n + 1 = 4k - 1$. First suppose that $m \neq n$.

LEMMA 3. *If $m \neq n$ then $M(f_1, f_2)$ is a topological sphere. The invariant $\lambda(M(f_1, f_2))$ is zero if m, n are not of the form $4r - 1$. If $m = 4r - 1$, $n = 4(k - r) - 1$, then*

$$\lambda \equiv \pm p_r(f_1) p_{k-r}(f_2) s_r s_{k-r}/s_k \pmod 1.$$

Proof. We may assume that $m < n$. The exact sequence

$$\pi_m(SO_n) \to \pi_m(SO_{n+1}) \to \pi_m(S^n) = 0$$

implies that f_1 is homotopic to a map f_1' which carries S^m into the subset $SO_n \subset SO_{n+1}$. According to Lemma 1 the manifold $M(f_1', f_2)$ is homeomorphic to S^{m+n+1}. But it can be verified that $M(f_1, f_2)$ is homeomorphic to $M(f_1', f_2)$, and therefore is also homeomorphic to the sphere.

Next consider the manifold W constructed in Section 1. Recall that W is the union of a fibre bundle over S^{m+1} with fibre D^{n+1} and a fibre bundle over S^{n+1} with fibre D^{m+1}. Call these sets W_2 and W_3 respectively, Thus $W_2 \cup W_3$ is W and $W_2 \cap W_3$ is a topological cell.

These bundles have canonical cross-sections corresponding to the center point of the disk. Hence S^{m+1} and S^{n+1} are imbedded in W. It follows easily that W has the same homology groups as $S^{m+1} \vee S^{n+1}$ (the union with a single point in common). That is $H_i(W; Z)$ is infinite cyclic for i equal to 0, $m + 1$, or $n + 1$, and zero otherwise.

The homology intersection ring of W (see Lefschetz [14]) is described as follows. Let a and b stand for generators in dimensions $n + 1$, $m + 1$ respectively. Clearly a and b have intersection number ± 1. The self-inter-

sections $a \cdot a$ and $b \cdot b$ are zero. For example $a \cdot a$ is represented by a cycle of dimension

$$\dim a + \dim a - \dim W = n - m$$

which lies on the sphere $S^{n+1} \subset W_3$. Since $H_{n-m}(S^{n+1}; Z) = 0$, this cycle is homologous to zero.

Applying Poincaré duality it follows that *$H^*(W, M; Z)$ is free abelian on three generators, say α in dimension $m+1$, β in dimension $n+1$, and $\alpha\beta$ in dimension $m+n+2$. The cup products $\alpha\alpha$ and $\beta\beta$ are zero.* This implies that the index $I(W)$ is zero.

Computation of the Pontrjagin numbers of W. We may assume that $m = 4r - 1$, $n = 4k - 4r - 1$. (If the dimensions are not of this form, then the Pontrjagin numbers are certainly zero, hence $\lambda \equiv 0$.) First consider the tangent bundle of W_2. This splits into a Whitney sum $\xi \oplus \eta$, where ξ is the bundle of vectors tangent to the fibre and η is the bundle of vectors normal to the fibre. Restricting η to the sphere $S^{m+1} \subset W_2$ we obtain the tangent bundle of S^{m+1} with trivial Pontrjagin classes. Restricting ξ to S^{m+1} we obtain the bundle determined by $(f_1) \in \pi_m(SO_{n+1})$. Thus $p_r(W_2) = p_r(\xi)$ is equal to the integer $p_r(f_1)$ multiplied by a generator of the infinite cyclic group $H^{4r}(W_2; Z)$. Using the isomorphisms

$$H^{4r}(W_2; Z) \leftarrow H^{4r}(W; Z) \xleftarrow{\ j\ } H^{4r}(W, M; Z)$$

it follows that

$$p_r(W) = \pm\, p_r(f_1)\, j(\alpha).$$

Similarly

$$p_{k-r}(W) = \pm\, p_{k-r}(f_2)\, j(\beta).$$

Thus *the Pontrjagin number* $(j^{-1}p_r)(j^{-1}p_{k-r})[W]$ *is equal to* $\pm\, p_r(f_1) p_{k-r}(f_2)$. All other Pontrjagin numbers of W are zero (except $(j^{-1}p_k)[W]$ which is not defined).

Computation of the coefficients of $p_r p_{k-r}$ in the Hirzebruch polynomial L_k. Define the symmetric function $\sum t_1^{i_1} \cdots t_a^{i_a}$ in indeterminates $t_1, \cdots, t_N$ as the sum of all monomials which can be obtained from $t_1^{i_1} \cdots t_a^{i_a}$ by permuting $t_1, \cdots, t_N$. Each possible monomial should be included only once in the sum. (For example $\sum t_1^r = t_1^r + \cdots + t_N^r$.) Hirzebruch showed [5] that the coefficient of $p_{i_1} \cdots p_{i_a}$ in L_k can be expressed in the form $\sum t_1^{i_1} \cdots t_a^{i_a}$, where $t_1, \cdots, t_N$ are certain fixed complex numbers. (Here N stands for

[5] See [4] § 1.4.1.

some fixed integer greater than or equal to k.) In particular, the coefficient s_k of p_k is equal to $\sum t_1^k$.

The product rule

$$(\sum t_1^r)(\sum t_1^{k-r}) = \sum t_1^k + \sum t_1^r t_2^{k-r} \qquad \text{for } r \neq k-r$$

is easily verified. Hence *the coefficient* $\sum t_1^r t_2^{k-r}$ *of* $p_r p_{k-r}$ *in* L_k *is equal to* $s_r s_{k-r} - s_k$.

Thus we have $I(W) = 0$ and

$$L_k(j^{-1}p_1, \cdots, j^{-1}p_{k-1}, 0)[W] = \pm p_r(f_1) p_{k-r}(f_2)(s_r s_{k-r} - s_k).$$

Dividing by s_k and reducing modulo one, this yields the required formula

$$\lambda(M) \equiv \pm p_r(f_1) p_{k-r}(f_2) s_r s_{k-r}/s_k \pmod 1$$

Now consider the case $m = n$. Again it is necessary to assume that m has the form $4r-1$ in order to obtain a non-trivial λ.

LEMMA 4. *If the maps f_1, f_2 both carry S^m into the subgroup $SO_m \subset SO_{m+1}$, then the formula*

$$\lambda(M) \equiv p_r(f_1) p_r(f_2) s_r s_r / s_{2r}$$

holds, just as in Lemma 3.

Proof. Just as above, $H_*(W;Z)$ is isomorphic to $H_*(S^{m+1} \vee S^{m+1})$. If $b, a \in H_{m+1}(W;Z)$ are the generators corresponding to the two spheres, then the intersection number $a \cdot b$ is ± 1. The hypothesis $f_1(S^m) \subset SO_m$ implies that the normal bundle of the first $(m+1)$-sphere in W has a cross-section. Hence the self-intersection number $a \cdot a$ is zero. Similarly $b \cdot b = 0$. It follows that W has index zero.

The computation of Pontrjagin classes for W proceeds as before. Thus

$$p_r(W) = \pm p_r(f_1) j\alpha \pm p_r(f_2) j\beta.$$

However the Pontrjagin number $(j^{-1}p_r)^2[W]$ is now equal to $\pm 2p_r(f_1)p_r(f_2)$. On the other hand, the coefficient of $p_r p_r$ in L_{2r} is equal[5] to $\frac{1}{2}(s_r s_r - s_{2r})$. Thus the factor of $\frac{1}{2}$ cancels the 2, so that

$$\lambda(M(f_1 f_2)) \equiv \pm p_r(f_1) p_r(f_2) s_r s_r / s_{2r}$$

as before.

In order to make use of Lemmas 3, 4 it is necessary to know what integers $p_r(f)$ can occur.

THEOREM OF BOTT [2], [3]. *In the stable range $q \geqq 4r$ the Pontrjagin homomorphism*

$$p_r\colon \pi_{4r-1}(SO_q) \to Z$$

has image generated by

$$(2r-1)! \text{ if } r \text{ is even}$$

$$2(2r-1)! \text{ if } r \text{ is odd.}$$

For smaller values of q this result can be augmented as follows.

LEMMA 5. *If $q \leqq 2r$ then the homomorphism p_r is zero. If $q > 2r$ then p_r is non-zero. In fact there exists an element*

$$(f) \in \pi_{4r-1}(SO_q)$$

such that the prime factors of $p_r(f)$ are all less than $2r$.

Proof by descending induction on q. Suppose that the assertion has been proved for $q+1$, and that $q > 2r$. In the exact sequence

$$\pi_{4r-1}(SO_q) \to \pi_{4r-1}(SO_{q+1}) \to \pi_{4r-1}(S^q),$$

the third group is stable. According to Serre [9] a prime π can divide the order of this group only if $2\pi - 3$ is less than or equal to the difference $4r - q - 1$. The inequalities $2\pi - 3 \leqq 4r - q - 1$, $q > 2r$, yield $\pi \leqq r$. Thus any element of $\pi_{4r-1}(SO_{q+1})$, after being multiplied by primes less than or equal to r, can be lifted back to $\pi_{4r-1}(SO_q)$. This completes the induction.

If $q < 2r$, then the Pontrjagin class p_r of any SO_q-bundle is zero. If $q = 2r$, then $p_r(\xi^{2r})$ is the square of the Euler class of ξ^{2r}. (See Borel and Serre [1].) Since our base space is S^{4r}, this implies that $p_r(\xi^{2r}) = 0$; which completes the proof of Lemma 5.

Combining Lemmas 3, 4, 5 this proves:

THEOREM 1. *Suppose that r is an integer satisfying*

$$k/3 < r \leqq k/2.$$

Then there exists a differentiable manifold M homeomorphic to S^{4k-1} for which $\lambda(M)$ is congruent modulo 1 *to $s_r s_{k-r}/s_k$ times some integer with prime factors all less than $2(k-r)$.*

The proof is straightforward. (The inequality $k/3 < r$ guarantees the existence of a map $f_2\colon S^{4(k-r)-1} \to SO_{4r}$ such that $p_{k-r}(f_2) \neq 0$.)

Note. Given k, the inequality $k/3 < r \leqq k/2$ has a solution r providing that $k = 2$ or $k \geqq 4$. It has no solution for $k = 1$ or 3.

THEOREM 2. *There exist at least 7 distinct differentiable structures on S^7; at least:*

$$\begin{array}{rl} 127 & \textit{on the 15-sphere,} \\ 73 & \textit{on the 19-sphere,} \\ 23 \cdot 89 \cdot 691 & \textit{on the 23-sphere,} \\ 8191 & \textit{on the 27-sphere, and at least} \\ 31 \cdot 151 \cdot 3617 & \textit{on the 31-sphere.} \end{array}$$

Proof. These results follow immediately from Theorem 1. As an example, for $k = 5$, taking $r = 2$, we have

$$s_2 s_3 / s_5 = 341/365.$$

Cancelling all prime factors less than 6 from the denominator, this leaves 73. But if M is a 19-manifold such that the denominator of $\lambda(M)$ is 73, then the first 73 manifolds

$$S^{19}, M, M \# M, M \# M \# M, \cdots$$

must be pairwise distinct. (Alternatively, if the homotopy class (f_1) is replaced by $q(f_1)$, $0 \leqq q < 73$, then we obtain 73 different values for the invariant λ.) Each one represent a possible differentiable structure for the 19-sphere.

In conclusion, here are two unsolved problems.

Problem 1. Does Theorem 1 imply the existence of non-standard differentiable structures on S^{4k-1} for all $k \geqq 4$? I have checked this only for k up to 14.

Problem 2. Is the invariant $\lambda(M^{4k-1})$ of a homotopy sphere always a multiple of the invariant

$$\lambda(M_0^{4k-1}) \equiv 8/s_k?$$

This question is of interest since, for any manifold M^{4k-1} which bounds a parallelizable manifold W, we have

$$\lambda(M^{4k-1}) \equiv I(W)/s_k \pmod 1,$$

and it can be shown that $I(W)$ is a multiple of 8. (Compare [7].)

REFERENCES.

[1] A. Borel and J. P. Serre, "Groupes de Lie et puissances réduites de Steenrod," *American Journal of Mathematics*, vol. 75 (1953), pp. 409-448.

[2] R. Bott, "The space of loops on a Lie group," *Michigan Mathematical Journal*, vol. 5 (1958), pp. 35-61.

[3] ——— and J. Milnor, "On the parallelizability of the spheres," *Bulletin of the American Mathematical Society*, vol. 64 (1958), pp. 87-89.

[4] F. Hirzebruch, *Neue topologische Methoden in der algebraischen Geometrie*, Springer, 1956.

[5] J. Milnor, "On manifolds homeomorphic to the 7-sphere," *Annals of Mathematics*, vol. 64 (1956), pp. 399-405.

[6] ———, "On the relationship between differentiable manifolds and combinatorial manifolds," (mimeographed), Princeton University, 1956.

[7] ———, "Differentiable manifolds which are homotopy spheres," (mimeographed), Princeton University, 1959.

[8] ———, "On the cobordism ring Ω^*, and a complex analogue," (in preparation).

[9] J. P. Serre, "Homologie singulière des espaces fibrés," *Annals of Mathematics*, vol. 54 (1951), pp. 425-505.

[10] N. Shimada, "Differentiable structures on the 15-sphere and Pontrjagin classes of certain manifolds," *Nagoya Mathematical Journal*, vol. 12 (1957), pp. 59-69.

[11] N. Steenrod, *The topology of fibre bundles*, Princeton, 1951.

[12] I. Tamura, "Homeomorphy classification of total spaces of sphere bundles over spheres," *Journal of the Mathematical Society of Japan*, vol. 10 (1958), pp. 29-43.

[13] R. Thom, "Les classes caractéristiques de Pontrjagin des variétés triangulées," *Topología Algebraica*, Mexico, 1958, pp. 54-67.

[14] S. Lefschetz, *Topology*, New York, Chelsea, 1956.

THE PRINCIPAL THREE-DIMENSIONAL SUBGROUP AND THE BETTI NUMBERS OF A COMPLEX SIMPLE LIE GROUP.*[1]

By Bertram Kostant.

1. Introduction.

1. Let $\mathfrak{g}$ be a complex simple Lie algebra and let G be the adjoint group of $\mathfrak{g}$. It is by now classical that the Poincaré polynomial $p_G(t)$ of G factors into the form,

$$p_G(t) = \prod_{i=1}^{l} (1 + t^{d_i}), \tag{1.1.1}$$

where l is the rank of $\mathfrak{g}$ and the d_i are odd integers. In this paper the integers m_i (elsewhere, sometimes $m_i + 1$) defined by $d_i = 2m_i + 1$ will be called the exponents of $\mathfrak{g}$. No doubt one of the reasons the problem of finding the exponents turned out to be as difficult as it was, is that there was no way known by which these numbers could be determined from a direct examination of the structure of $\mathfrak{g}$, particularly the root structure. The first procedure for extracting the exponents from the root structure of $\mathfrak{g}$ was found by R. Bott. The proof of the validity of this procedure depends upon Morse theory.[2] A second and much simpler way, which we shall presently describe, of "reading off" the exponents from the root structure of $\mathfrak{g}$ was discovered by Arnold Shapiro. (It is interesting that Shapiro discovered the procedure by misinterpreting the method of Bott.) However, even though one verifies that the numbers produced by this procedure agree with the exponents, unlike the case with Bott's method, the important question of proving that this "agreement" is more than just a coincidence remained open. The procedure is as follows: Let Δ^+ be the set of positive roots relative to some Weyl chamber in a Cartan subalgebra of $\mathfrak{g}$. If $\phi \in \Delta^+$ let $o(\phi)$ be the sum of the coefficients of ϕ relative to the basis of simple positive roots. Let b_k be the number of roots ϕ such that $o(\phi) = k$. Then $b_k - b_{k+1}$ is the number of times k occurs as an exponent of $\mathfrak{g}$. For example, if we apply this to the case where

* Received December 19, 1958.

[1] Research supported by Air Force Contract AF 49(638)-79.

[2] See R. Bott, "An application of the Morse theory to the topology of Lie groups," *Bull. Soc. Math. France*, t. 84 (1956), pp. 251-281.

$\mathfrak{g}$ is Lie algebra of the special linear group $SL(n,C)$ then the fact that the number of matrix units e_{ij} such that $j-i=k$, where $1\leq k\leq n-1$, is greater by one then the number of matrix units e_{ij} such that $j-i=k+1$ accounts for the fact that the exponents of $\mathfrak{g}$ are $1,2,\cdots,n-1$.

After Shapiro informed us of this counting device for the exponents we observed that it could be reformulated as follows: The principal three-dimensional subalgebra $\mathfrak{a}_0$ of $\mathfrak{g}$ is a uniquely defined (up to conjugacy) three dimensional simple subalgebra (TDS) of $\mathfrak{g}$ which can be readily distinguished from other TDS by its properties. [It was discovered almost simultaneously by Dynkin and de Siebenthal (see [6] and [13]) and later used extensively by these authors (see e.g. [7])]. Using standard facts in the representation theory of a TDS it is not difficult to show that the observation of Shapiro is equivalent to the observation that if we decompose the adjoint representation of $\mathfrak{a}_0$ on $\mathfrak{g}$ into a direct sum of irreducible representations then the number of irreducible components is l and the dimensions of these components are d_i, $i=1,2,\cdots,l$, where the d_i are given by (1.1.1). However, this reformulation of the procedure still does not supply a proof.

A second empirical procedure for finding the exponents was discovered by H. M. Coxeter. He recognized that the exponents can be obtained from a particular transformation γ in the Weyl group, which he had been studying, and which we take the liberty of calling a Coxeter-Killing transformation, in the following manner (see [5]): Let h be the order of γ. Coxeter observed that (1) h satisfies $hl=2r$, where r is the number of positive roots, (2) $m_i\leq h$ for all i and (3) the eigenvalues of γ are ω^{m_i}, $i=1,2,\cdots,l$, where $\omega=e^{2\pi i/h}$. A proof of (2) and (3) would provide, among other things, a proof of duality in the exponents m_i observed by Chevalley (see [3], p. 24) since non-real eigenvalues of γ necessarily occur in conjugate pairs. Requiring (1) $hl=2r$ as the only empirically observed fact such a proof was recently obtained by A. J. Coleman (see [4]). A proof that $hl=2r$ will be given in this paper. A second question posed in [4] of showing that $h=1+o(\psi)$, where ψ is the highest root, will also be settled here.

It will be the main result of this paper to establish a direct relationship between the principal TDS, its adjoint representation of $\mathfrak{g}$, and the transformation of Coxeter-Killing. The proof that the procedure of Shapiro yields the exponents is then a direct consequence of this relationship. A major role here is played by a particular conjugate class in G, the elements of which we call principal elements of G. It is shown that an element of G which induces a transformation of Coxeter-Killing on a Cartan subalgebra is necessarily a principal element. On the other hand a principal element of G

belongs to the subgroup corresponding to a principal TDS and is sufficiently specialized in that subgroup so that the adjoint representation of a principal TDS on $\mathfrak{g}$ is determined by its eigenvalues. That the conjugate class of principal elements is truly a distinguished one in G may be judged from the following characterization (one of several) of principal elements. Let A be an arbitrary regular element of G. Let k be the order of A (possibly ∞). Then $k \geqq h$ and $k = h$ if and only A is principal.

An important role is also played here by two distinguished classes of $\mathfrak{g}$, the elments of which we have, respectively, called principal nilpotent and cyclic (the latter name is derived from the transformation properties of such elements in the case when $\mathfrak{g}$ is the Lie algebra of $SL(n, C)$). As is the case with the principal elements of G these elements can be given simple characterizations (Corollary 5.3, Theorem 9.2 and Corollary 9.3).

In this paper §§ 1-4 are devoted to the theory of the general TDS. The main theorems here are Theorems 3.6 and 4.2. Both concern conjugacy questions. The first is an extension of a well known theorem of Jacobson-Morosov. A corollary of it puts the conjugate classes of TDS in $\mathfrak{g}$ in a canonical one-one correspondence with the conjugate classes of nilpotent elements in $\mathfrak{g}$. The second is implicit in the proof of a weaker theorem of Malcev.

In § 5 the theory of the principal TDS is taken up. For the most part the theorems here are devoted to characterizing principal TDS among all TDS and principal nilpotent elements among all nilpotent elements. The result here which is used most often in the remainder of the paper is Corollary 5.3.

The main results of the paper are given in §§ 6-9.

2. Preliminaries and the complex three dimensional simple Lie algebra.

1. Let $\mathfrak{g}$ be a complex semi-simple Lie algebra. Let n and l be respectively the dimension and rank of $\mathfrak{g}$. As usual the linear transformation

$$y \to [x, y]$$

is designated by $\operatorname{ad} x$ and $x \to \operatorname{ad} x$ is the adjoint representation of $\mathfrak{g}$ on itself. If $\mathfrak{u}$ is a Lie subalgebra of $\mathfrak{g}$ the mapping $x \to \operatorname{ad} x$ for $x \in \mathfrak{u}$ will be called the adjoint representation of $\mathfrak{u}$ on $\mathfrak{g}$. We distinguish two types of elements in $\mathfrak{g}$. An element $x \in \mathfrak{g}$ is called nilpotent if $\operatorname{ad} x$ is nilpotent and is called semi-simple if $\operatorname{ad} x$ is completely reducible, that is, (since we are dealing with

complex numbers) if $\operatorname{ad} x$ is diagonizable.[3] Only the zero element is both nilpotent and semi-simple.

We recall that any element x contained in a Cartan subalgebra $\mathfrak{h} \subseteq \mathfrak{g}$ is necessarily semi-simple and conversely every semi-simple element may be embedded in a Cartan subalgebra. (See e.g. [8], p. 119).

For any element $x \in \mathfrak{g}$ let $\mathfrak{g}^x$ designate the kernel of $\operatorname{ad} x$. We recall that x is called regular when x is semi-simple and $\mathfrak{g}^x$ is a Cartan subalgebra.

2.2. Let G designate the adjoint group of $\mathfrak{g}$. Since this is the only group associated with $\mathfrak{g}$ that we shall consider the operation of exponentiation (Exp) will be always understood to go from $\mathfrak{g}$ to G.

Elements x and y in $\mathfrak{g}$ are called conjugate if there exists $A \in G$ such that $Ax = y$.

2.3. The simplest complex semi-simple Lie algebra (up to isomorphism) is $\mathfrak{a}_1$, the Lie algebra of all complex 2×2 matrices of trace zero. In this case $n = 3$ and $l = 1$. One knows that any three dimensional complex semi-simple Lie algebra is isomorphic to $\mathfrak{a}_1$.

By conjugating any element of $\mathfrak{a}_1$ into Jordan canonical form the following is apparent:

(a) every non-zero element in $\mathfrak{a}_1$ is either semi-simple or nilpotent,

(b) the set of all non-zero nilpotent elements in $\mathfrak{a}_1$ form a single conjugate class,

(c) if $x, y \in \mathfrak{a}_1$ are semi-simple, $x \neq 0$, then y is conjugate to a unique, up to sign, scalar multiple of x. (Note also that the set of non-zero semi-simple elements coincides with the set of regular elements in $\mathfrak{a}_1$).

2.4. Let $\mathfrak{a}$ be a 3-dimensional complex simple Lie algebra. We recall further facts in the structure theory of $\mathfrak{a}$. Let $x \in \mathfrak{a}$ be a regular element. Then the eigenvalues of $\operatorname{ad} x$ are a, $0 - a$ for some non-zero complex number a. We may modify x by scalar multiplication so that a and $-a$ take the values 1 and -1. This defines x uniquely up to conjugacy. We thus isolate a particular conjugate class in $\mathfrak{a}$. We thus isolate a particular conjugate class in $\mathfrak{a}$. The elements in this class will be called mono-semisimple.

Let $x \in \mathfrak{a}$ be a mono-semisimple element. Let $e_+ \in \mathfrak{a}$ be a non-zero eigen-

[3] It is not difficult to show that this very same definition [of semi-simple and nilpotent elements] may be achieved using any faithful representation of $\mathfrak{g}$ in place of the adjoint representation. This follows, e.g., from Lemma 5.4 and well known facts in the representation theory of $\mathfrak{g}$.

vector of $\operatorname{ad} x$ for the eigenvalue 1; e_+ is unique up to a non-zero scalar. Then e_-, an eigenvector of $\operatorname{ad} x$ for the value -1, is uniquely determined by condition $[e_+, e_-] = x$. One thus has the commutation relations

$$(2.4.1) \qquad \begin{aligned} &(1) \quad [x, e_+] = e_+ \\ &(2) \quad [x, e_-] = -e_- \\ &(3) \quad [e_+, e_-] = x \end{aligned}$$

for the basis x, e_+, e_- of $\mathfrak{a}$.

2.5. When $\mathfrak{a} = \mathfrak{a}_1$ the elements x, e_+, and e_- may be realized by the matrices

$$x = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix}, \qquad e_+ = 2^{-\frac{1}{2}} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad e = 2^{-\frac{1}{2}} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

For each positive integer d there exists up to equivalence one and only one linear irreducible representation of $\mathfrak{a}$ having that dimension. (For a complete treatment of the representation theory of $\mathfrak{a}_1$ see [12, Exposé no. 10].) To describe an irreducible representation π_d of $\mathfrak{g}$ on a d-dimensional vector space V first define the number k by the relation $d = 2k + 1$. It is of course to be noted that k is an integer if and only if d is odd. We may then find a basis v_j, $j = k, k-1, \cdots, -k$ of V, where the vectors are each unique up to a scalar factor, satisfying the following condition:

$$\pi_d(x) v_j = j \cdot v_j.$$

The behavior of $\pi_d(e_+)$ and $\pi_d(e_-)$ on the one dimensional spaces (v_j) is given by

$$\pi_d(e_+)(v_j) = (v_{j+1})$$
$$\pi_d(e_-)(v_j) = (v_{j-1})$$

where $v_{k+1} = v_{-k-1} = 0$. Thus v_j is an eigenvector for $\pi_d(e_+)\pi_d(e_-)$ and $\pi_d(e_-)\pi_d(e_+)$, where in fact

$$\pi_d(e_+)\pi_d(e_-) v_j = \tfrac{1}{2}(k - j + 1)(k + j) v_j$$

and

$$\pi_d(e_-)\pi_d(e_+) v_j = \tfrac{1}{2}(k - j)(k + j + 1) v_j.$$

It follows that with respect to the ordering $v_k, v_{k-1}, \cdots, v_{-k}$ of the basal elements, when the latter are suitably modified by scalar multiplication, one obtains for $\pi_d(x)$, $\pi_d(e_+)$ and $\pi_d(e_-)$ the matrices

$$\pi_d(x) = \begin{vmatrix} k & & & & 0 \\ & k-1 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ 0 & & & & -k \end{vmatrix}$$

$$\pi_d(e_+) = 2^{-\frac{1}{2}} \begin{vmatrix} 0 & (1(2k))^{\frac{1}{2}} & & & & 0 \\ & 0 & (2(2k-1))^{\frac{1}{2}} & & & \\ & & 0 & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & \cdot & \\ & & & & 0 & (2k(1))^{\frac{1}{2}} \\ 0 & & & & & 0 \end{vmatrix}$$

$$\pi_d(e_-) = 2^{-\frac{1}{2}} \begin{vmatrix} 0 & & & & & 0 \\ (1(2k))^{\frac{1}{2}} & 0 & & & & \\ & (2(2k-1))^{\frac{1}{2}} & 0 & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & \cdot & \\ & & & & 0 & \\ 0 & & & & (2k(1))^{\frac{1}{2}} & 0 \end{vmatrix}.$$

Several facts are to be noted. Among those we shall require are

(a) The dimension d of V is odd or even according as the eigenvalues of $\pi_d(x)$ are all integers or all half-integers.[4]

(b) The eigenvalues of $\pi_d(x)$ all occur with multiplicity 1 and the real number j is an eigenvalue of $\pi_d(x)$ if and only if $d-(2\,|\,j\,|+1)$ is a non-negative even integer.

(c) The number k, where $2k+1=d$, may be characterized as the highest eigenvalue of $\pi_d(x)$. Furthermore, the one-dimensional eigenspace for this eigenvalue k may be characterized as the kernel of $\pi_d(e_+)$.

Now assume π is an arbitrary, not necessarily irreducible, representation of $\mathfrak{a}$ on the finite-dimensional vector space V. One knows π may be decomposed into a direct sum of irreducible representations. It follows then that one knows π up to equivalence as soon as the dimensions of the irreducible components of π are given. That is, if n_k denotes the number of such components having dimension $2k+1$, then π is given when the sequence n_k, $k=0,\frac{1}{2},1,\cdots$, is known.

[4] We use the word half-integer to designate all numbers of the form $m+\frac{1}{2}$, where m is an integer.

(d) The problem of finding the sequence n_k can be reduced to an investigation of the kernel $W \subseteq V$ of $\pi(e_+)$. In fact, it follows from (c) that

$$\dim W = n_0 + n_{\frac{1}{2}} + n_1 + \cdots.$$

Furthermore W is stable under $\pi(x)$ and if $w \in W$ is any eigenvector of $\pi(x)$, w may be embedded in an irreducible component of π. Hence if $k_1, k_2, \cdots, k_p$ are the eigenvalues of $\pi(x)$ on W, the dimensions of the irreducible components of π are respectively $2k_1 + 1, 2k_2 + 1, \cdots, 2k_p + 1$. (Note that the k_i are non-negative.)

(e) The space V admits a canonical direct sum decomposition

$$V = V^E + V^O,$$

where V^E is spanned by eigenvectors of $\pi(x)$ belonging to half-integral eigenvalues and V^O is spanned by eigenvectors of $\pi(x)$ belonging to integral eigenvalues. It follows immediately from (a) that V^E and V^O are both stable subspaces for the representation π and that in the complete reduction of $\pi | V^E$ only irreducible representations of even dimension appear and the complete reduction of $\pi | V^O$ yields only irreducible representations of odd dimension.[5]

(f) Now let V_j be the eigenspace of $\pi(x)$ for the eigenvalue j. Clearly $\dim V_j = \dim V_{-j}$. Furthermore, if j is non-negative, it follows from (b) that

$$\dim V_j = n_j + n_{j+1} + n_{j+2} + \cdots.$$

The statement (f) has the following 2 consequences:

(g) The dimension of V_0, that is the dimension of the kernel of $\pi(x)$ (nullity of $\pi(x)$), equals $n_0 + n_1 + n_2 + \cdots$.

(h) If j is non-negative,

$$\dim V_j - \dim V_{j+1} = n_j.$$

Finally, we shall require

(i) If k is the maximal eigenvalue of $\pi(x)$,

$$V = \sum_{p=-2k}^{2k} V_{p/2}$$

is a direct sum and $\sum_{p=1}^{2k} V_{p/2}$ lies in the range of $\pi(e_+)$.

[5] If π is a representation on a vector space V and $U \subset V$ is stable under π, then $\pi | U$ denotes the representation on U obtained by restricting π to U.

3. Nilpotent elements and TDS.

1. Let $\mathfrak{g}$ be a complex semi-simple Lie algebra. Consider the question of determining all three dimensional simple subalgebras (TDS) in $\mathfrak{g}$. If $\mathfrak{a} \subseteq \mathfrak{g}$ is a TDS, then by considering the adjoint representation of $\mathfrak{a}$ on $\mathfrak{g}$ it follows from the representation theory of $\mathfrak{a}$ outlined in § 2.5 that any nilpotent element of $\mathfrak{a}$ is necessarily nilpotent in $\mathfrak{g}$ and any semi-simple element of $\mathfrak{a}$ is a semi-simple element of $\mathfrak{g}$ (Also see footnote 3). Since $\mathfrak{a}$ has only semi-simple and nilpotent elements (see § 2.3(a)), the question arises (1) which nilpotent and semi-simple elements of $\mathfrak{g}$ can be embedded in a TDS and (2) how does one find all such subalgebras. We shall first consider the case of nilpotent elements.

A theorem of Morosov asserts that every nilpotent element of $\mathfrak{g}$ can be embedded in a TDS. (See [11].) However, his proof was incomplete. Later in [9] Jacobson gave a correct proof of this result. Since the proof leads into Theorem 3.6, we shall give it here. The proof requires Lemma 3.3. With the exception of the proof of Lemma 3.3 the proof is the same as the one given by Jacobson.

3.2. A famous result of Jacobson asserts that if A and B are linear transformations on a finite dimensional space V with the condition that $[A,B]$ commutes with A, then $[A,B]$ is nilpotent. If in addition A is assumed nilpotent, the following lemma (which is no doubt known) asserts that AB is nilpotent.

LEMMA 3.2. *Let A and B be linear transformations on a finite dimensional space V. Assume A is nilpotent and*

$$[A,[A,B]]=0.$$

Then AB is nilpotent.

Proof. Let V^k be the kernel of A^k. We wish to show AB leaves V^k invariant. The result is obvious if $k=0$. Assume the result is known to be true for $k=r$. Let $x \in V^{r+1}$

$$ABx = [A,B]x + BAx.$$

Apply A^{r+1} to both sides. Then

$$\begin{aligned} A^{r+1}(AB)x &= [A,B]A^{r+1}x + A^{r+1}BAx \\ &= 0 + A^r(AB)Ax. \end{aligned}$$

But $Ax \in V^r$ and by our assumption $(AB)Ax \in V^r$. Thus $A^r(AB)Ax = 0$. Hence $ABx \in V^{r+1}$.

Assume AB is not nilpotent. Then there exists a scalar λ, $\lambda \neq 0$ and a vector $x \in V$, $x \neq 0$ such that

$$ABx = \lambda x. \tag{3.2.1}$$

Let k be the smallest integer such that $x \in V^{k+1}$.

Now

$$A^k ABx = A^k[A, B]x + A^k BAx.$$

But $A^k B = BA^k + k[A, B]A^{k-1}$. Thus

$$A^k BAx = BA^{k+1}x + k[A, B]A^k x$$
$$= 0 + k[A, B]A^k x.$$

Hence

$$A^k ABx = (k+1)[A, B]A^k x.$$

But by (3.21)

$$A^k ABx = \lambda A^k x.$$

Hence $[A, B]A^k x = (\lambda/k + 1)A^k x$.

Since $A^k x \neq 0$, this contradicts Jacobson's lemma asserting the nilpotence of $[A, B]$. Q. E. D.

3.3. Now for any $x, y \in \mathfrak{g}$ let

$$(x, y) = \operatorname{tr} \operatorname{ad} x \operatorname{ad} y$$

be the Cartan-Killing bilinear form B on $\mathfrak{g}$. Using the non-singularity of B on $\mathfrak{g}$ we can now prove the following lemma. Lemma 3.3 is crucial in the proof that any nilpotent element $e \in \mathfrak{g}$ can be embedded in a TDS of $\mathfrak{g}$.

It is clear that if e is contained in a TDS then e must lie in the range of $(\operatorname{ad} e)^2$ since according to § 2.3(b), e can play the role of e_+ in the commutation relations (2.4.1). In particular, it is interesting enough to observe then that for any non-zero nilpotent element e, $(\operatorname{ad} e)^2 \neq 0$. (The degree of nilpotency of $\operatorname{ad} e$ is greater than 2.)

LEMMA 3.3. *Let $e \in \mathfrak{g}$ be a nilpotent element. Then e is in the range of $(\operatorname{ad} e)^2$.*

Proof. The invariance of B under the adjoint representation implies that, for any $z \in \mathfrak{g}$, $\operatorname{ad} z$ is skew-symmetric with respect to B and hence $(\operatorname{ad} z)^2$ is symmetric. In particular, this is true for $z = e$. But now if A is a symmetric operator (with respect to B) on $\mathfrak{g}$ and if R_A and K_A are, respectively, the range and kernel of A, then

$$(R_A, K_A) = 0$$

By the non-singularity of B, then, to show an element z lies in R_A, it suffices to show $(z, y) = 0$ for all $y \in K_A$. Letting $A = (\mathrm{ad}\, e)^2$, to prove the lemma it suffices to show that

$$[e, [e, y]] = 0 \tag{3.3.1}$$

implies

$$(e, y) = 0.$$

But under the adjoint representation (3.3.1) becomes

$$[\mathrm{ad}\, e, [\mathrm{ad}\, e, \mathrm{ad}\, y]] = 0.$$

Since $\mathrm{ad}\, e$ is nilpotent, we apply Lemma 3.2 to assert that $\mathrm{ad}\, e\, \mathrm{ad}\, y$ is nilpotent. But then by definition of B it is clear that $(e, y) = 0$. Q.E.D.

3.4. By Lemma 3.3, e may be written as

$$[[f, e], e] = e \tag{3.4.1}$$

for some $f \in \mathfrak{g}$. Let $x = [f, e]$ so that $[x, e] = e$.

LEMMA 3.4. *Let $\mathfrak{g}^e$ be the kernel of* $\mathrm{ad}\, e$. *Then $\mathfrak{g}^e$ is invariant under* $\mathrm{ad}\, x$. *Furthermore if m is the smallest integer such that* $(\mathrm{ad}\, e)^{m+1} = 0$, *then*

$$\prod_{p=0}^{m} (\mathrm{ad}\, x - p/2)$$

vanishes on $\mathfrak{g}^e$.

Proof. The space $(\mathrm{ad}\, e)^p \mathfrak{g}$ is the range of $(\mathrm{ad}\, e)^p$. We define a sequence of subspaces $\mathfrak{d}_p$ of $\mathfrak{g}^e$, $p = 0, 1, \cdots, m+1$, where

$$\mathfrak{g}^e = \mathfrak{d}_0 \supseteq \mathfrak{d}_1 \supseteq \cdots \supseteq \mathfrak{d}_{m+1} = 0, \tag{3.4.2}$$

by letting

$$\mathfrak{d}_p = (\mathrm{ad}\, e)^p \mathfrak{g} \cap \mathfrak{g}^p.$$

First observe that $\mathfrak{g}^e$ is invariant under $\mathrm{ad}\, x$. Indeed, if $y \in \mathfrak{g}^e$,

$$\begin{aligned} [e, [x, y]] &= [[e, x], y] \\ &= -[e, y] \\ &= 0. \end{aligned}$$

We now show that

$$(\mathrm{ad}\, x - p/2) : \mathfrak{d}_p \to \mathfrak{d}_{p+1}. \tag{3.4.3}$$

Let $y \in \mathfrak{d}_p$. Then $y = (\mathrm{ad}\, e)^p z$ for some $z \in \mathfrak{g}$. Now since $[x, e] = e$ clearly

$$[\mathrm{ad}\, x, (\mathrm{ad}\, e)^p] = p(\mathrm{ad}\, e)^p.$$

Thus

$$[\operatorname{ad} x, (\operatorname{ad} e)^p]z = py,$$

or

$$\begin{aligned}[x,y] - p\cdot y &= (\operatorname{ad} e)^p[x,z] \\ &= (\operatorname{ad} e)^p[[f,e]z] \qquad (3.4.4)\\ &= (\operatorname{ad} e)^{p+1}[z,f] + (\operatorname{ad} e)^p \operatorname{ad} f[e,z].\end{aligned}$$

But

$$\begin{aligned}[(\operatorname{ad} e)^p, \operatorname{ad} f] &= -\sum_{i=0}^{p-1} (\operatorname{ad} e)^i \operatorname{ad} x (\operatorname{ad} e)^{p-1-i} \\ &= \tfrac{1}{2}p(p-1)(\operatorname{ad} e)^{p-1} - p \operatorname{ad} x (\operatorname{ad} e)^{p-1}.\end{aligned}$$

Applying this to $[e,z]$ we obtain

$$\begin{aligned}(\operatorname{ad} e)^p \operatorname{ad} f[e,z] &= \operatorname{ad} f(\operatorname{ad} e)^p[e,z] \\ &\quad + \tfrac{1}{2}p(p-1)(\operatorname{ad} e)^p z - p[x, (\operatorname{ad} e)^p z] \\ &= [f,[e,y]] + \tfrac{1}{2}p(p-1)y - p[x,y] \\ &= \tfrac{1}{2}p(p-1)y - p[x,y].\end{aligned}$$

But then (3.3.4) becomes

$$(p+1)[x,y] - \tfrac{1}{2}p(p+1)y = (\operatorname{ad} e)^{p+1}[z,f]$$

or

$$[x,y] - \tfrac{1}{2}py \in \mathfrak{d}_{p+1}.$$

This proves (3.4.3). It then follows immediately from (3.4.2) that

$$\prod_{p=0}^{m} (\operatorname{ad} x - p/2)$$

vanishes on $\mathfrak{g}^e$. Q.E.D.

It is an immediate consequence of Lemma 3.4 that $\operatorname{ad} x$ is completely reducible on $\mathfrak{g}^e$ and that its eigenvalues are restricted to non-negative integers and half-integers. In particular, what is essential for us at this point is

COROLLARY 3.4. *The linear transformation* $\operatorname{ad} x + 1$ *is non-singular on* $\mathfrak{g}^e$.

We can now prove

THEOREM 3.4 (Jacobson-Morosov). *Every nilpotent element of a complex semi-simple Lie algebra can be embedded in a* TDS.

Proof. Let e be nilpotent, $e \neq 0$, and let f and x be defined as in § 3.4.[6]

[6] The theorem holds when $e = 0$ once we know the existence of a single TDS. The existence of a TDS follows from the proof since g contains non-zero nilpotent elements.

In case $[x,f] = -f$ we would be done, that is, x, e, f would satisfy the desired commutation relations. The problem is to modify f so that this relation is satisfied without destroying the relation (3.4.1). Even if $[x,f]+f \neq 0$ we still have

$$[[x,f]+f, e] = 0$$

as one easily checks. Thus $[x,f]+f \in \mathfrak{g}^e$. But now by Corollary 3.4, since $\operatorname{ad} x + 1$ is non-singular on $\mathfrak{g}^e$, there exists a unique $g \in \mathfrak{g}^e$ such that

$$[x,f]+f = [x,g]+g.$$

Then writing e_+ for e and letting $e_- = f - g$ it follows that

$$\begin{aligned} &[x, e_+] = e_+ \\ (3.4.5) \qquad &[x, e_-] = -e_- \\ &[e_+, e_-] = x. \end{aligned}$$

This proves Theorem 3.4 as soon as one notes that x, e_+ and e_- must be linearly independent.

3.5. Any set of non-zero elements x, e_+ and e_- in $\mathfrak{g}$ satisfying the commutation relations (3.4.5) will henceforth be called an S-triple (to be written $\{x, e_+, e_-\}$). The element x will be called the neutral element of the S-triple and e_+ (resp. e_-) will be called the nil-positive (resp. nil-negative) element of the S-triple. It is obvious that the elements of an S-triple form a basis of a TDS. Two S-triples are called conjugate if there exists $A \in G$ which carries one set onto the other.

Given a non-zero nilpotent element $e \in \mathfrak{g}$ we wish now to find all S-triples which contain e as the nil-positive element. (By § 2.3(b) this yields all TDS which contain e).

First we note the following corollary of the proof of Theorem 3.4.

COROLLARY 3.5. *Let $e \in \mathfrak{g}$ be nilpotent, $e \neq 0$, then x and e are respectively the neutral and nil-positive elements of an* S-triple *if and only if* (1) *x is in the range of* $\operatorname{ad} e$ *and* (2) *$[x, e] = e$. Furthermore if x and e satisfy these conditions such an* S-triple *system is unique* (*and hence x and e are contained in just one* TDS).

Proof. The first part of Corollary 3.5 follows from the proof of Theorem 3.4 and the definition of x used in the proof (see (3.4.1)). To prove the uniqueness of the nil-negative element assume that $\{x, e, f_1\}$ and $\{x, e, f_2\}$ are two S-triples. It is obvious then that

$$[e, f_1 - f_2] = 0$$

and hence $f_1 - f_2 \in \mathfrak{g}^e$. But

$$[x, f_1 - f_2] + f_1 - f_2 = 0$$

so that $f_1 - f_2$ is an eigenvector of $\operatorname{ad} x + 1$ on $\mathfrak{g}^e$. By this implies $f_1 = f_2$.
Q. E. D.

3.6. As a consequence of Corollary 3.5 the problem of finding all S-triple systems containing e as the nil-positive element reduces to finding all elements $x \in \mathfrak{g}$ which satisfy the conditions of Corollary 3.5. Towards this end define, for $e \in \mathfrak{g}$, the subspace

$$\mathfrak{g}_e = \operatorname{ad} e(\mathfrak{g}) \cap \mathfrak{g}^e,$$

the intersection of the range and kernel of $\operatorname{ad} e$. We now observe that $\mathfrak{g}_e$ is a Lie subalgebra of $\mathfrak{g}$. Indeed, $\mathfrak{g}^e$ is a Lie subalgebra of $\mathfrak{g}$. Therefore it sufficies only to show that $[u, v] \in \operatorname{ad} e(\mathfrak{g})$ if $u, v \in \mathfrak{g}_e$. Writing $v = [e, w]$ we have, since $u \in \mathfrak{g}^e$,

$$\begin{aligned}[u, v] &= [u, [e, w]] \\ &= [e, [u, w]].\end{aligned}$$

This proves $[u, v] \in \mathfrak{g}_e$. Now let G_e be the subgroup of G corresponding to the subalgebra $\mathfrak{g}_e$. Note that among other things the elements of G_e leave e fixed. We can now state

THEOREM 3.6. *Let $e \in \mathfrak{g}$, $e \neq 0$, be nilpotent. Let $\mathfrak{g}_e$ and G_e be as above. Then the elements of $\mathfrak{g}_e$ are all nilpotent (and hence the elements in G_e are unipotent). Let $x \in \mathfrak{g}$ be such that x and e are, respectively, the neutral and nil-positive elements of an* S-triple. *Then the linear coset $x + \mathfrak{g}_e$ of $\mathfrak{g}_e$ is the set of all neutral elements taken from all* S-triples *containing e as nil-positive element. Furthermore, any two elements in $x + \mathfrak{g}_e$ are conjugate. Moreover the conjugation can be performed by an element in G_e so that e is fixed under the conjugation. In fact for any $A \in G_e$, $Ax \in x + \mathfrak{g}_e$ and the map*

$$G_e \to x + \mathfrak{g}_e$$

defined by making A, $A \in G_e$, correspond to Ax is one-one and onto.

In other words (recalling Corollary 3.5) if $\{x, e, f\}$ is the S-triple *containing x and e, the map*

$$A \to \{Ax, e, Af\}$$

sets up a one-one correspondence of the group G_e onto the set of all S-triples *containing e as nil-positive element. Furthermore Ax ranges over $x + \mathfrak{g}_e$.*

Proof. Assume $\{x, e, f\}$ and $\{y, e, g\}$ are S-triples and e nil-positive in both cases while x and y are neutral.

Since

$$[x, e] = [y, e] = e,$$

it follows that $y - x \in \mathfrak{g}^e$. But clearly $[e, g - f] = y - x$. That is, $y - x \in \operatorname{ad} e(\mathfrak{g})$. Hence $y - x \in \mathfrak{g}_e$ or $y \in x + \mathfrak{g}_e$. Conversely, if $y \in x + \mathfrak{g}_e$, then clearly $[y, e] = e$ and $y \in \operatorname{ad} e(\mathfrak{g})$. Thus applying Corollary 3.5 y *is* a neutral element of an S-triple containing e.

Now according to Lemma 3.4 $\mathfrak{g}^e$ admits the direct decomposition

$$\mathfrak{g}^e = \sum_{p=0}^{m} \mathfrak{b}_{p/2},$$

where m is the smallest integer such that $(\operatorname{ad} e)^{m+1} = 0$ and $\mathfrak{b}_{p/2}$ is the eigenspace of $\operatorname{ad} x$ in $\mathfrak{g}^e$ belonging to the eigenvalue $p/2$. It is of course clear that

$$[\mathfrak{b}_{p/2}, \mathfrak{b}_{p'/2}] \subseteq \mathfrak{b}_{(p+p')/2}. \tag{3.6.1}$$

Let $\mathfrak{a}$ be the TDS spanned by x, e and f. Now if π_d is an irreducible representation of $\mathfrak{a}$ on a vector space of dimension d it is clear from § 2.5(i) that the eigenspace belonging to the highest eigenvalue $(\frac{1}{2}(d-1))$, of $\pi_d(x)$ lies in the range of $\pi_d(e)$ if and only if $d \geqq 2$. Now decompose $\mathfrak{g}$ into irreducible subspaces under the adjoint representation of $\mathfrak{a}$ on $\mathfrak{g}$ and apply this fact to the irreducible components. Recalling 2.5(d) it becomes clear then that the subspace $\mathfrak{g}_e$ of $\mathfrak{g}^e$ can be written

$$\mathfrak{g}_e = \sum_{p=1}^{m} \mathfrak{b}_{p/2} \tag{3.6.2}$$

and hence, in particular, $\operatorname{ad} x$ is non-singular on $\mathfrak{g}_e$.

One immediate observation from (3.6.1) and (3.6.2) is that $\mathfrak{g}_e$ is a nilpotent Lie subalgebra of $\mathfrak{g}$. Furthermore, since the eigenvalues of $\operatorname{ad} x$ on $\mathfrak{g}_e$ are strictly positive it is clear from a relation similar to (3.6.1) that $\operatorname{ad} w$ is nilpotent for every $w \in \mathfrak{g}_e$.[7] That is, the elements of $\operatorname{ad} \mathfrak{g}_e$ may be simultaneously triangulized with zeros appearing along the diagonal for every element. It follows then from well known facts concerning linear nilpotent Lie algebras that in such a case G_e is closed, simply connected—that is, G_e is homeomorphic to Euclidean space—and the exponential map

$$\operatorname{Exp}: \mathfrak{g}_e \to G_e$$

[7] That is, if $\mathfrak{g}_j$ is the eigenspace of $\operatorname{ad} x$ on $\mathfrak{g}$ for the eigenvalue j then clearly $[\mathfrak{g}_j, \mathfrak{b}_i] \subset \mathfrak{g}_{i+j}$.

is one-one and onto. That is, every $A \in G_e$ may be uniquely written $A = \operatorname{Exp} w$ for a unique $w \in \mathfrak{g}_e$. But then

$$(3.6.3) \qquad Ax = x + [w, x] + \tfrac{1}{2}[w[w, x]] + \cdots.$$

Since $\mathfrak{g}_e$ is stable under $\operatorname{ad} x$ and since $\mathfrak{g}_e$ is a Lie subalgebra, all terms starting from the second on the right side of (3.6.3) lie in $\mathfrak{g}_e$ so that $Ax \in x + \mathfrak{g}_e$.

Now let $v \in \mathfrak{g}_e$. Assume that there exists a unique element $w_j \in \mathfrak{g}_e$ such that (1)

$$w_j \in \sum_{p=1}^{j} \mathfrak{b}_{p/2}$$

and (2)

$$\operatorname{Exp} w_j(x) - (x + v) \in \sum_{p=j+1}^{m} \mathfrak{b}_{p/2}.$$

Now let z_{j+1} be the component of $\operatorname{Exp} w_j(x) - (x + v)$ in $\mathfrak{b}_{(j+1)/2}$. Then if

$$w_{j+1} = w_j + (2/j + 1) z_{j+1}$$

it is clear that $[w_{j+1}, x] = [w_j, x] - z_{j+1}$. On the other hand, for $i > 1$ it follows from (3.6.1) that the components of $(\operatorname{ad} w_{j+1})^i x$ and $(\operatorname{ad} w_j)^i x$ in $\mathfrak{b}_{s/2}$ are the same for all $s \leqq j + 1$. Thus

$$w_{j+1} \in \sum_{s=1}^{j+1} \mathfrak{b}_{s/2}$$

and

$$\operatorname{Exp} w_{j+1}(x) - (x + v) \in \sum_{s=j+2}^{m} \mathfrak{b}_{s/2}$$

and furthermore that in satisfying these conditions w_{j+1} is unique. If we define $w_1 = -2v_{\frac{1}{2}}$, where $v_{\frac{1}{2}}$ is the component of v in $\mathfrak{b}_{\frac{1}{2}}$, then w_1 uniquely satisfies (1) and (2) when $j = 1$. Thus we have proved inductively that there exists a unique $w \in \mathfrak{g}_e$ such that

$$\operatorname{Exp} w(x) = x + v. \qquad \text{Q. E. D.}$$

Note. *It is useful to observe that the proof, above, of the statement that Ax ranges over $x + \mathfrak{g}_e$ when A ranges over G_e depends essentially on just two facts,* (1), *the nilpotence of $\mathfrak{g}_e$ and* (2), *the non-singularity of* $\operatorname{ad} x$ *on $\mathfrak{g}_e$.*

We can now supplement Theorem 3.4 with

COROLLARY 3.6. *Let $e \in \mathfrak{g}$ be nilpotent, $e \neq 0$, and assume $e \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, where $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are two* TDS. *Then $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are conjugate to each other. Furthermore, the conjugation can be chosen so as to leave e fixed.*

Proof. According to § 2.3 (b) we may find two S-triples each containing e as nil-positive element and which, respectively, are bases for $\mathfrak{a}_1$ and $\mathfrak{a}_2$. Corollary 3.6 then follows immediately from Theorem 3.6. Q. E. D.

3.7. Corollary 3.6 is actually just a special case of the following corollary. The set of all TDS in $\mathfrak{g}$ breaks up into conjugate classes under the action of G. Concerning these classes we have

COROLLARY 3.7. *The conjugate classes of* TDS *in* $\mathfrak{g}$ *are in a natural one-one correspondence with the conjugate classes of non-zero nilpotent elements in* $\mathfrak{g}$. *The correspondence is established by associating to the conjugate class of* $\mathfrak{a}$, *a* TDS *in* $\mathfrak{g}$, *the conjugate class of any non-zero nilpotent element in* $\mathfrak{a}$. *That is, two* TDS $\mathfrak{a}_1$ *and* $\mathfrak{a}_2$ *are conjugate if and only if* e_1 *and* e_2 *are conjugates, where* $e_1 \in \mathfrak{a}_1$, $e_2 \in \mathfrak{a}_2$ *and* e_1, e_2 *are non-zero nilpotent elements.*

Proof. Follows immediately from § 2.3 (b), Theorem 3.4 and Corollary 3.6. Q. E. D.

4. Semi-simple elements and TDS.

1. We now consider the semi-simple elements of a TDS and take up questions of conjugacy. Let $\{x, e_+, e_-\}$ be an S-triple with x and e_+, respectively, as the neutral and nil-positive elements. We wish first to determine all S-triples which contain x (necessarily as neutral element). Let $\mathfrak{a}$ be the TDS spanned by x, e_+ and e_-. By considering the adjoint representation of $\mathfrak{a}$ on $\mathfrak{g}$ it follows from § 2.5 that the eigenvalues of $\operatorname{ad} x$ on $\mathfrak{g}$ are integers and half-integers. In fact, recalling § 2.5 (f) and § 2.5 (i), if $\mathfrak{g}_{p/2}$ is the eigenspace of $\operatorname{ad} x$ for the eigenvalue $p/2$ and if k is the maximal value of $\operatorname{ad} x$, then

$$\dim \mathfrak{g}_{p/2} = \dim \mathfrak{g}_{-p/2}$$

and

$$\mathfrak{g} = \sum_{p=-2k}^{2k} \mathfrak{g}_{p/2}.$$

In this case, however, we have the addtiional relation

$$[\mathfrak{g}_{p/2}, \mathfrak{g}_{p'/2}] \subseteq \mathfrak{g}_{(p+p')/2}. \tag{4.1.1}$$

Since we are concerned with S-triples containing x, interest focuses on $\mathfrak{g}_1$ since any nil-positive element in an S-triple containing x obviously belongs to $\mathfrak{g}_1$. In particular, $e_+ \in \mathfrak{g}_1$. The question arises which other elements of $\mathfrak{g}_1$

belong to S-triples containing x and whether such S-triples are conjugate to $\{x, e_+, e_-\}$. To settle this question we first consider $\mathfrak{g}_0 = \mathfrak{g}^x$.

It follows immediately from (4.1.1) that $\mathfrak{g}^x$ is a Lie subalgebra. Let G^x be the subgroup of the adjoint group corresponding to the subalgebra $\mathfrak{g}^x$. It also follows from (4.1.1) that each of the subspaces $\mathfrak{g}_{p/2}$ is stable under the adjoint representation of $\mathfrak{g}^x$ on $\mathfrak{g}$ and hence these spaces must be stable under G^x. We are particularly interested in the action of G^x on $\mathfrak{g}_1$.

4.2. Now for each element $e \in \mathfrak{g}_1$ it follows from (4.1.1) that

$$\operatorname{ad} e : \mathfrak{g}_0 \to \mathfrak{g}_1.$$

Let T_e be the restriction of $\operatorname{ad} e$ to $\mathfrak{g}_0$. Our interest now centers on what will be shown to be an important subset of $\mathfrak{g}_1$. Define

$$\hat{\mathfrak{g}}_1 = \{e \in \mathfrak{g}_1 \mid T_e \text{ maps } \mathfrak{g}_0 \text{ onto } \mathfrak{g}_1\}.$$

That is, $e \in \hat{\mathfrak{g}}_1$ if and only if the rank of T_e equals the dimensions of $\mathfrak{g}_1$.

We now observe

LEMMA 4.2A. *A necessary condition that an element $e \in \mathfrak{g}_1$ be the nil-positive element of an S-*triple *containing x is that $e \in \hat{\mathfrak{g}}_1$. In particular, $e_+ \in \hat{\mathfrak{g}}_1$.*

Proof. Indeed, assume e and x belong to an S-triple. Let $\mathfrak{a}'$ be the TDS which contains e and x. If we apply § 2.5(i) to the adjoint representation of $\mathfrak{a}$ on $\mathfrak{g}$ it follows that $\mathfrak{g}_1$ is the range of $\operatorname{ad} e$. On the other hand, it is clear from (4.1.1) that $\operatorname{ad} e(\mathfrak{g}) \cap \mathfrak{g}_1 = \operatorname{ad} e(\mathfrak{g}_0) \cap \mathfrak{g}_1$. Hence T_e must map $\mathfrak{g}_0$ onto $\mathfrak{g}_1$. Q. E. D.

The following topological properties of $\hat{\mathfrak{g}}_1$ are needed for the proof of Theorem 4.2 (Here one is inspired by the use of regular elements in the usual proof of the conjugacy of any two Cartan subalgebras.).

LEMMA 4.2B. *The set $\hat{\mathfrak{g}}_1$ is an open, dense and connected subset of $\mathfrak{g}_1$.*

Proof. It follows from Lemma 4.2A that $\hat{\mathfrak{g}}_1$ is not empty ($e_+ \in \hat{\mathfrak{g}}_1$). Choose a basis of $\mathfrak{g}_0$ and a basis of $\mathfrak{g}_1$. For any $e \in \mathfrak{g}_1$ set $T_e{}^0$ equal to the $\dim \mathfrak{g}_0 \times \dim \mathfrak{g}_1$ matrix determined by T_e and the given pair of bases. It is clear then that $\hat{\mathfrak{g}}_1$ is the set of all $e \in \mathfrak{g}_1$ such that at least one $\dim \mathfrak{g}_1 \times \dim \mathfrak{g}_1$ minor of $T_e{}^0$ is not zero. But it is an easily verified general fact that if F_j, $j = 1, 2, \cdots, m$, are m non-zero polynomials on a complex vector space V then the complement $\hat{V}$ to the set of common zeros in V of all the F_j is open, dense and connected. Indeed, if $u \in \hat{V}$ and $v \in V$, then there are only a finite

number of complex scalars λ such that $F_j^0(\lambda) = F_j(\lambda u + (1-\lambda)v)$ vanishes for at least one j. Q. E. D.

Now observe that $\hat{\mathfrak{g}}_1$ is invariant under G^x. The major point in the proof of Theorem 3.4 is the observation contained in the following lemma.

LEMMA 4.2C. *Let $e \in \hat{\mathfrak{g}}_1$; then the orbit $G^x e$ of e under the action of G^x is an open subset of $\mathfrak{g}_1$ (and hence of $\hat{\mathfrak{g}}_1$).*

Proof. The mapping $A \to Ae$ of G^x into $\mathfrak{g}_1$ is analytic. Thus it suffices to show that the differential of this mapping carries the tangent space to G^x at 1 *onto* the tangent space of $\mathfrak{g}_1$ at e. But the image of the former, under the differential, when translated to the origin of $\mathfrak{g}_1$ is just the subspace $\operatorname{ad}\mathfrak{g}^x(e)$ of $\mathfrak{g}_1$. But $\mathfrak{g}^x = \mathfrak{g}_0$ and since $e \in \hat{\mathfrak{g}}_1$, this space coincides with $\mathfrak{g}_1$, by definition of $\hat{\mathfrak{g}}_1$. Thus $G^x e$ is open in $\mathfrak{g}_1$. Q. E. D.

We have shown $G^x e$ is open in $\hat{\mathfrak{g}}_1$ for any $e \in \hat{\mathfrak{g}}_1$. But for $e_1, e_2 \in \mathfrak{g}_1$, $G^x e_1$ and $G^x e_2$ are the same sets or else they are disjoint. But this fact taken together with Lemma 4.2B (the latter asserting the connectivity of $\hat{\mathfrak{g}}_1$) implies that there can be at most one orbit. That is, $\hat{\mathfrak{g}}_1$ is itself a single orbit of G^x.

But then recalling Lemma 4.2A and observing that x is fixed under the action of G^x we see that the following theorem has been proved.

THEOREM 4.2. *Let $x \in \mathfrak{g}$ be the neutral element of an S-*triple *$\{x, e_+, e_-\}$. (See § 3.5.) As in § 2.1 let $\mathfrak{g}^x$ be the centralizer of x in $\mathfrak{g}$ and let G^x be the subgroup of G corresponding to $\mathfrak{g}^x$.*

Define

$$\mathfrak{g}_1 = \{e \in \mathfrak{g} \mid [x, e] = e\}.$$

Then

$$\operatorname{ad} e\colon \mathfrak{g}^x \to \mathfrak{g}_1 \tag{4.2.1}$$

for any $e \in \mathfrak{g}_1$.

*Let $e \in \mathfrak{g}$. Then e and x are, respectively, the nil-positive and neutral elements of an S-*triple *if and only if (1) $e \in \mathfrak{g}_1$ and (2) the map (4.2.1) is onto. Moreover, any two S-*triples *which contain x are conjugate to each other and the conjugation can be performed by an element in G^x.*

In other words, if

$$\hat{\mathfrak{g}}_1 = \{e \in \mathfrak{g}_1 \mid (4.2.1) \text{ is an onto map}\}$$

then $\hat{\mathfrak{g}}_1$ is the conjugate class of e_+ under the action of G^x. That is

$$\hat{\mathfrak{g}}_1 = G^x e_+.$$

*Furthermore, $\hat{\mathfrak{g}}_1$ coincides with the set of all nil-positive elements taken from all S-*triples *having x as neutral element.*

The statement of Theorem 4.2 gives a complete and simple description of the set of all nil-positive elements which "go" with a given neutral element. However, it is implicitly contained in Malcev's proof of the following corollary. Furthermore our proof of Theorem 4.2 although found without knowledge of Malcev's proof of Corollary 4.2 (yet with the knowledge that it had been proved) amounts to only a technical simplification of Malcev's proof.

Corollary 4.2 provides the basis by which all the TDS in any complex simple Lie algebra have been classified (see [7], § 8).

COROLLARY 4.2 (Malcev). *Two* TDS *in $\mathfrak{g}$ are conjugate if and only if any mono-semisimple element of one is conjugate to any mono-semisimple element of the other* (see [10]).

4.3. Now, continuing with the notation of § 4.1 and § 4.2, the subset $\hat{\mathfrak{g}}_1$ in $\mathfrak{g}_1$ is of course only a part of the conjugate class of e_+ in $\mathfrak{g}$. It does not seem likely that one can give a simple description of the entire class. Nevertheless, it is easy to describe a part of this class which is yet larger than $\hat{\mathfrak{g}}_1$ (see Theorem 4.3, Theorem 4.3 is required for the proof of Theorem 5.3) and we shall do this now.

For any $t = 0, 1, \cdots, 2k$ let

$$\mathfrak{n}_{t/2} = \sum_{p=t}^{2k} \mathfrak{g}_{p/2}.$$

It is clear from (4.1.1) that $\mathfrak{n}_{t/2}$ is a Lie subalgebra of $\mathfrak{g}$. Let $N_{t/2}$ be the subgroup of G corresponding to $\mathfrak{n}_{t/2}$. We now have, in terms if the preceding notation,

THEOREM 4.3. *The orbits $N_0 x$ and $N_0 e_+$ of e_+ and x under the action of the group N_0 are as follows:*

$$N_0 x = x + \mathfrak{n}_{\frac{1}{2}}$$

and

$$N_0 e_+ = \hat{\mathfrak{g}}_1 + \mathfrak{n}_{\frac{3}{2}}.$$

In fact, G^x is a subgroup of N_0 and $N_{\frac{1}{2}}$ is a normal subgroup of N_0. Moreover, the elements of $N_{\frac{1}{2}}$ are unipotent linear transformations of $\mathfrak{g}$. Furthermore, N_0 can be written as a semi-direct product

$$N_0 = N_{\frac{1}{2}} G^x$$

(every element $C \in N_0$ is uniquely written $C = AA'$, where $A \in N_{\frac{1}{2}}$, $A' \in G^x$) and the correspondence

$$A \to Ax$$

sets up a one-one mapping of $N_{\frac{1}{2}}$ onto $x + \mathfrak{n}_{\frac{1}{2}}$ while the correspondence

$$A \to Ae_+$$

defines a mapping of N_0 onto $e_+ + \mathfrak{n}_{\frac{3}{2}}$.

Proof. Since $\mathfrak{n}_0 = \mathfrak{g}^x + \mathfrak{n}_{\frac{1}{2}}$ is a semi-direct sum (that is, $[\mathfrak{g}^x, \mathfrak{n}_{\frac{1}{2}}] \subseteq \mathfrak{n}_{\frac{1}{2}}$) it follows that every element $C \in N_0$ can be written, $C = AA'$, where $A \in N_{\frac{1}{2}}$ and $A' \in G^x$. On the other hand, if $A \in N_{\frac{1}{2}}$ and $y \in \mathfrak{g}_{t/2}$, then $Ay = y + w$, where $w \in \sum_{p=t+1}^{2k} \mathfrak{g}_{p/2}$. This implies A is unipotent. It also implies that $N_{\frac{1}{2}} \cap G^x = (1)$ and hence N_0 is a semi-direct product of $N_{\frac{1}{2}}$ and G^x. Now observe that $\mathfrak{n}_{\frac{1}{2}}$ is stable under $\operatorname{ad} x$ and $\operatorname{ad} x$ is non-singular on $\mathfrak{n}_{\frac{1}{2}}$. The proof that the correspondence $A \to Ax$ sets up a one-one mapping of $N_{\frac{1}{2}}$ onto $x + \mathfrak{n}_{\frac{1}{2}}$ then proceeds in essentially the same way as the proof of Theorem 3.6 (Recall that $[\mathfrak{n}_{t/2}, \mathfrak{n}_{t'/2}] \subseteq \mathfrak{n}_{(t+t')/2}$ and see the note following Theorem 3.6) and we shall not repeat it. On the other hand, one cannot claim that the mapping of $N_{\frac{1}{2}}$ into $e_+ + \mathfrak{n}_{\frac{3}{2}}$ defined by the correspondence $A \to Ae$ is one-one. This is because $\operatorname{ad} e_+$ annihilates non-zero elements in $\mathfrak{n}_{\frac{1}{2}}$. But $\operatorname{ad} e_+$ maps $\mathfrak{g}_{p/2}$ into $\mathfrak{g}_{(p/2)+1}$ and applying 2.5(i) to the adjoint representation of $\mathfrak{a}$ on $\mathfrak{g}$ it follows that

$$\operatorname{ad} e_+ : \mathfrak{n}_{\frac{1}{2}} \to \mathfrak{n}_{\frac{3}{2}}$$

is an onto mapping. Proceeding then in a manner similar to the proof of Theorem 3.6 it follows easily that $N_{\frac{1}{2}}$ is mapped onto $e_+ + \mathfrak{n}_{\frac{3}{2}}$ by the correspondence $A \to Ae_+$. Q. E. D.

As we have remarked, Corollary 4.2 has provided the basis by which the conjugate classes of TDS have been classified (See [7], § 8). That is if x is a mono-semisimple element of a TDS, we know that x is a semi-simple element of $\mathfrak{g}$ and that the eigenvalues of $\operatorname{ad} x$ are real (in fact are integers and half-integers). To classify the conjugate classes of TDS it suffices then by Corollary 4.2 to find a fundamental domain for the action of G on the set of semi-simple x in $\mathfrak{g}$ such that $\operatorname{ad} x$ has real eigenvalues and determine which in the domain are mono-semisimple elements of TDS. The Weyl chamber is such a domain and we shall presently consider it.

(In view of Corollary 3.7 for the purposes of classifying conjugate classes of TDS it might be well to look for natural representative elements for the

conjugate classes of nilpotent elements. To my knowledge no such investigation has been undertaken).

5. The principal TDS.

1. Let $\mathfrak{h} \subseteq \mathfrak{g}$ be a Cartan subalgebra which we shall assume is fixed once and for all. Let Δ be the set of roots with respect to $\mathfrak{h}$ and let e_ϕ, $\phi \in \Delta$ be representative root vectors so that we have usual direct sum decomposition

$$\mathfrak{g} = \mathfrak{h} + \sum_{\phi \in \Delta} (e_\phi).$$

Since B is non-isngular on $\mathfrak{h}$, we may assume Δ is embedded in $\mathfrak{h}$. That is, if $\phi \in \Delta$, then ϕ may be identified with an element in $\mathfrak{h}$ by the relation

$$[x, e_\phi] = (x, \phi) e_\phi.$$

for all $x \in \mathfrak{h}$. One knows then if e_ϕ and $e_{-\phi}$ are normalized only in so far as

$$(e_\phi, e_{-\phi}) = 1, \tag{5.1.0}$$

as we shall assume, then

$$[e_\phi, e_{-\phi}] = \phi. \tag{5.1.1}$$

Now let $\mathfrak{h}^\#$ be the real linear space in $\mathfrak{h}$ spanned by the roots. One knows that

$$\mathfrak{h} = \mathfrak{h}^\# + i\mathfrak{h}^\#$$

is a real direct sum. We recall that B is positive definite on $\mathfrak{h}^\#$ (see e. g. [12], p. 10-04). In particular then, (x, ϕ) is real for all $x \in \mathfrak{h}^\#$ at all $\phi \in \Delta$. This means $\mathfrak{h}^\#$ can be characterized as the set of all elements $x \in \mathfrak{h}$ such that $\operatorname{ad} x$ has real eigenvalues.

Hereafter, if Y is any subset of $\mathfrak{h}$, we will let $Y^\# = Y \cap \mathfrak{h}^\#$.

Now for any $\phi \in \Delta$ let

$$\mathfrak{h}[\phi] = \{x \in \mathfrak{h} \mid (\phi, x) = 0\}.$$

Then, clearly, if R is the set of all regular elements in $\mathfrak{h}$,

$$R^\# = \mathfrak{h} - \bigcup_{\phi \in \Delta} \mathfrak{h}[\phi].$$

The connected components of $R^\#$ are called open Weyl chambers. Now assume a lexicographical ordering is given in $\mathfrak{h}^\#$. Let Δ^+ (resp. Δ^-) be the set of positive roots (resp. negative roots). The ordering distinguishes a particular open Weyl chamber D^0 which can be defined by

$$D^0 = \{x \in \mathfrak{h}^\# \mid (\phi, x) > 0 \text{ for all } \phi \in \Delta^+\}.$$

The closure D of D^0 is called a Weyl chamber. It can be defined in the same way as D^0 except that one replaces the strict inequality $>$ by the inequality $\geqq$. The set D is a fundamental domain for the action of G on the set of all semi-simple elements y in $\mathfrak{g}$ such that $\operatorname{ad} y$ has real eigenvalues. That is, if y is such an element there exists one and only one ([12], p. 16-08 and [7], Lemma 8.2) element x in D which is conjugate to y.

Now let $\Pi = \{\alpha_1, \alpha_2, \cdots, \alpha_l\}$ be the set of simple positive roots. The simple positive roots form a basis of $\mathfrak{h}$ and for every root ϕ, upon writing

$$\phi = \sum_{i=1}^{l} n_i \alpha_i,$$

one knows that the coefficients n_i are integers which are all non-negative or all non-positive according as $\phi \in \Delta^+$ or $\phi \in \Delta^-$. We define the order $o(\phi)$ of ϕ by letting

$$o(\phi) = \sum_{i=1}^{l} n_i. \tag{5.1.2}$$

Obviously, if ϕ_1, ϕ_2 and $\phi_1 + \phi_2 \in \Delta$, then

$$o(\phi_1 + \phi_2) = o(\phi_1) + o(\phi_2). \tag{5.1.3}$$

Let ϵ_i, $i = 1, 2, \cdots, l$, be the dual basis in h to the α_j. Since

$$(\epsilon_i, \alpha_j) = \delta_{ij}, \tag{5.1.4}$$

it is clear that $\epsilon_i \in D$. More generally, if

$$x = \sum_{i=1}^{l} a_i \epsilon_i, \tag{5.1.5}$$

then $x \in D$ if and only if $a_i \geqq 0$, $i = 1, 2, \cdots, l$. Indeed,

$$(x, \alpha_i) = a_i. \tag{5.1.6}$$

Now assume $x \in D$ is the neutral element of an S-triple $\{x, e_+, e_-\}$. Since the eigenvalues of $\operatorname{ad} x$ are integral multiples of $\frac{1}{2}$, it follows from that in the expansion (5.1.5) $a_i = \frac{1}{2} m_i$ for some non-negative integer m_i. On the other hand, it is not possible for a_i to be greater than 1. Indeed, since $\operatorname{ad} x(e_-) = -e_-$, it is clear that

$$e_- = \sum_{\phi \in \Delta^-} c_\phi e_\phi,$$

where we emphasize the summation is over negative roots. Hence it follows from § 2.5(d) (with signs reversed. Also see Lemma 3.4) that if $a_i > 1$, $\operatorname{ad} e_-(e_{\alpha_i})$ is a non-zero eigenvector of $\operatorname{ad} x$ with the positive eigenvalue $a_i - 1$.

But then since $x \in D$, this implies $[e_{-}, e_{\alpha_i}]$ is a sum of root vectors for positive roots. This, however, clearly contradicts the simplicity of α_i. We have proved then that $a_i = 0, \frac{1}{2}$, or 1 for $i = 1, 2, \cdots, l$. More than this we have (see [7], Theorem 8.3).

LEMMA 5.1. *Let the Weyl chamber D and the basis ϵ_i, $i = 1, 2, \cdots, l$ of $\mathfrak{h}$ be given as above. Assume that $x \in D$ is a mono-semisimple element of a* TDS. *Then*

$$x = \sum_{i=1}^{l} a_i \epsilon_i,$$

where for each $i = 1, 2, \cdots, l$, we have $a_i = 0$, $\frac{1}{2}$, or 1. Furthermore, if $x_1, x_2, \cdots, x_b \in D$ is the set (ordered) of all elements in D which happen to be mono-semisimple elements in at least one TDS *(so that $b < 3^l$), then there are exactly b conjugate classes of* TDS *in $\mathfrak{g}$. In fact, if x_i is a mono-semisimple element of the* TDS *$\mathfrak{a}_i$ for $i = 1, 2, \cdots, b$, then the subalgebras $\mathfrak{a}_i$, $i = 1, 2, \cdots, b$, are representatives of the conjugate classes.*

For each simple Lie algebra $\mathfrak{g}$ Dynkin lists [7] which among the $3^l - 1$ choices are indeed mono-semisimple elements of a TDS.

5.2. We retain the notation of Lemma 5.1. Among the elements x_j, $j = 1, 2, \cdots, b$ there is a distinguished one. This is the case when $a_i = 1$, $i = 1, 2, \cdots, l$. That is, for one of the x_j all the a_i (in (5.15)) take the maximal possible value.

LEMMA 5.2. *Let D and ϵ_i, $i = 1, 2, \cdots, l$, be as defined in* 5.1. *Let $x_0 \in D$ be given by*

$$x_0 = \sum_{i=1}^{l} \epsilon_i. \tag{5.2.1}$$

Then x_0 is a mono-semisimple element of a TDS

Proof. Since the elements of α_i form a basis of $\mathfrak{h}^{\#}$, x_0 may be uniquely written

$$x_0 = \sum_{i=1}^{l} r_i \alpha_i.$$

Now let c_i, $i = 1, 2, \cdots, l$, be any l non-zero complex numbers. Define

$$e_0 = \sum_{i=1}^{l} c_i e_{\alpha_i} \tag{5.2.2}$$

and

$$f_0 = \sum_{i=1}^{l} (r_i / c_i) e_{-\alpha_i}. \tag{5.2.3}$$

Clearly $(\alpha_i, x_0) = 1$ for all i. Thus

$$[x_0, e_0] = e_0$$

and

$$[x_0 f_0] = -f_0.$$

On the other hand, since $\alpha_i - \alpha_j$ is never a root, it follows from (5.1.1) that

$$[e_0, f_0] = x_0$$

so that $\{x_0, e_0, f_0\}$ form a S-triple. Q. E. D.

Let x_0, e_0 and f_0 be as defined in the proof of Lemma 5.2. Let $\mathfrak{a}_0$ be the TDS spanned by the vectors. The TDS $\mathfrak{a}_0$ or any conjugate TDS is called (originally in [6]) a principal TDS of $\mathfrak{g}$. It and some of its properties were discovered by Dynkin and de Siebenthal (See [6] and [13]). We shall call the S-triple (or any of its conjugates) $\{x_0, e_0, f_0\}$ a principal S-triple. The matrices exhibited in § 2.5 are an example of a principal S-triple in the Lie algebra of $SL(d, C)$.

One of the first properties we observe about the neutral element of a principal S-triple is that it is regular. In fact, $x_0 \in \mathfrak{h}^{\#}$ and for any $\phi \in \Delta$ clearly

$$(x_0, \phi) = o(\phi) \neq 0 \tag{5.2.4}$$

(see (5.1.2)). We shall call x_0 or any element of $\mathfrak{g}$ conjugate to x_0 a principal regular element of $\mathfrak{g}$. Any element of the conjugate class of e_0 will be called a principal nilpotent element of $\mathfrak{g}$.

One of the most significant ways in which a principal TDS is distinguished among all TDS is in regard to its adjoint representation on $\mathfrak{g}$.

For any TDS $\mathfrak{a}$ of $\mathfrak{g}$ let $n(\mathfrak{a})$, $n^E(\mathfrak{a})$ and $n^O(\mathfrak{a})$ designate, respectively, the number of irreducible components occurring in the complete reduction of the adjoint representation of $\mathfrak{a}$ on $\mathfrak{g}$, the number having even dimension and the number having odd dimension.

THEOREM 5.2. *Let $\mathfrak{a}$ be any* TDS *of $\mathfrak{g}$. Then $n(\mathfrak{a}) \geqq l$. Furthermore $\mathfrak{a}$ is principal if and only if $n(\mathfrak{a}) = l$.*

Proof. Let $\{x, e, f\}$ be an S-triple whose linear span is $\mathfrak{a}$. In fact, employing the notation of § 5.1 we may assume $x \in D \subseteq \mathfrak{h}$. Since $\mathfrak{h}$ is contained in $\mathfrak{g}^x$ (see § 2.1), obviously $\dim \mathfrak{g}^x \geqq l$. But now according to 2.5(g) we have $n^O(\mathfrak{a}) = \dim \mathfrak{g}^x$. Thus

$$n(\mathfrak{a}) \geqq n^O(\mathfrak{a}) = \dim \mathfrak{g}^x \geqq l \tag{5.2.5}$$

which proves the first part of Theorem 5.2. Now if $\mathfrak{a}$ is principal x is regular and hence $\dim \mathfrak{g}^x = l$. On the other hand, in this case all the eigenvalues of $\operatorname{ad} x$ are integers (see (5.1.2)) so that $n^E(\mathfrak{a}) = 0$ (see § 2.5(e)). Thus if $\mathfrak{a}$ is principal, $n(\mathfrak{a}) = n^O(\mathfrak{a}) = l$. Now, conversely, assume $n(\mathfrak{a}) = l$. But then by (5.2.5) $\dim \mathfrak{g}^x = l$ which implies x is regular. Writing $x = \sum_{i=1}^{l} a_i \epsilon_i$ as in § 5.1, it follows then that $a_i = \frac{1}{2}$ or 1 for all i. But since $n^O(\mathfrak{a}) = n(\mathfrak{a})$, that is, $n^E(\mathfrak{a}) = 0$, this means (see § 2.5(e)) the eigenvalues of $\operatorname{ad} x$ are all integral. Thus $a_i \neq \frac{1}{2}$ by (5.1.6) and hence $x = \sum_{i=1}^{l} \epsilon_i$ so that $\mathfrak{a}$ is principal by Corollary 4.2. Q.E.D.

As a corollary of the proof we have

COROLLARY 5.2. *Let* $\mathfrak{a}$ *be any* TDS *of* $\mathfrak{g}$; *then* $n^O(\mathfrak{a}) \geqq l$. *Furthermore,* $n(\mathfrak{a})^O = l$ *if and only if the mono-semisimple elements of* $\mathfrak{a}$ *are regular in* $\mathfrak{g}$. *In case* $\mathfrak{a}$ *is principal* $n^E(\mathfrak{a}) = 0$.

5.3. The following corollary of Theorem 5.2 distinguishes the principal nilpotent elements in the set of all nilpotent elements in $\mathfrak{g}$. The proof follows immediately from § 2.5(d) and Theorem 5.2.

COROLLARY 5.3. *Let e be a nilpotent element in* $\mathfrak{g}$; *then* $\dim \mathfrak{g}^e \geqq l$ *and* $\dim \mathfrak{g}^e = l$ *if and only if e is principal nilpotent.*

Now let $\{x_0, e_0, f_0\}$ be the principal S-triple defined as in § 5.2. We will now apply the theory of § 4.1 to this S-triple.

First of all, since the eigenvalues of $\operatorname{ad} x_0$ are integral, we observe that $\mathfrak{g}_{p/2} = 0$ whenever $p/2$ is not an integer and for j a non-zero integer

$$\mathfrak{g}_j = \sum_{o(\phi)=j} (e_\phi) \tag{5.3.1}$$

and

$$\mathfrak{g}_0 = \mathfrak{h}.$$

We will write $\mathfrak{n}$ for $\mathfrak{n}_{\frac{1}{2}} = \mathfrak{n}_1$ and $\mathfrak{s}$ for $\mathfrak{n}_0$. Then

$$\mathfrak{n} = \sum_{\phi \in \Delta^+} (e_\phi)$$

(as is well known) is a maximal Lie subalgebra of nilpotent elements and $\mathfrak{s} = \mathfrak{h} + \mathfrak{n}$ is a maximal solvable Lie subalgebra of $\mathfrak{g}$. Let H, N and S be the subgroups of G corresponding to $\mathfrak{h}$, $\mathfrak{n}$ and $\mathfrak{s}$.

Recalling that

$$e_0 = \sum_{i=1}^{l} c_i e_{\alpha_i},$$

where $c_i \neq 0$, $i = 1, 2, \cdots, l$ it follows from Theorems 4.2 and 4.3 that in this case

$$He_0 = \hat{\mathfrak{g}}_1 = \{e \in \mathfrak{g}_1 \mid e = \sum_{i=1}^{l} a_{\alpha_i} e_{\alpha_i}, \text{ where } a_{\alpha_i} \neq 0,\ i = 1, 2, \cdots, l\}$$

and (since $\mathfrak{n}_{\frac{3}{2}} = \mathfrak{n}_2$)

$$Se_0 = \hat{\mathfrak{g}}_1 + \mathfrak{n}_2 = \{e \in \mathfrak{n} \mid e = \sum_{\phi \in \Delta^+} a_\phi e_\phi, \text{ where } a_\phi \neq 0 \text{ when } \phi = \alpha_i,\ i = 1, 2, \cdots, l\}. \tag{5.3.2}$$

We emphasize that (5.3.2) above implies that "almost all" the elements in the maximal subalgebra of nilpotent elements $\mathfrak{n}$ are principal nilpotent (and hence lie in a single conjugate class).

We wish to prove now that Se_0 contains every principal nilpotent in $\mathfrak{n}$, that is, we have the following simple characterization of those elements in $\mathfrak{n}$ which are principal nilpotent.

THEOREM 5.3. *Let $\mathfrak{n} \subseteq \mathfrak{g}$ be the maximal Lie subalgebra of nilpotent elements given by*

$$\mathfrak{n} = \sum_{\phi \in \Delta^+} (e_\phi).$$

Let $e \in \mathfrak{n}$,

$$e = \sum_{\phi \in \Delta^+} a_\phi e_\phi$$

be arbitrary. Then e is principal nilpotent if and only if $a_\phi \neq 0$ for $\phi = \alpha_i$, $i = 1, 2, \cdots, l$.

Proof. By (5.3.2) if e satisfies the condition stated in Theorem 5.3, then e is principal nilpotent. Conversely, let $e \in \mathfrak{n}$ be principal nilpotent and assume $a_{\alpha_j} = 0$, for some j.

Assume first that $\mathfrak{g}$ is simple. Let $\psi \in \Delta$ be the highest root. We recall two basic facts about the highest root. One, upon writing $\psi = \sum_{i=1}^{l} q_i \alpha_i$ the integers q_i satisfy

$$q_i \geqq 1 \tag{5.3.3}$$

and

$$o(\psi) > o(\phi) \tag{5.3.4}$$

for any $\phi \in \Delta$, $\phi \neq \psi$. Indeed, both of these facts are immediate consequences of the following single fact: If $\phi = \sum_{i=1}^{l} t_i \alpha_i$ is any root, then

$$t_i \leqq q_i \tag{5.3.5}$$

for $i=1,2,\cdots,l$. Finally, (5.3.5) is a consequence of well known facts in representation theory; in fact, the adjoint representation of $\mathfrak{g}$ is irreducible and by definition of ψ, e_ψ is the weight vector belonging to the highest weight, ψ. One knows then that e_ϕ, for any $\phi \in \Delta$, is obtained by applying polynomials (non-commutative) in the operators $\operatorname{ad} e_{-\alpha_i}$, $i=1,2,\cdots,l$, to e_ψ. This proves (5.3.5). Let

$$q=\sum_{i=1}^{l} q_i = o(\psi).$$

Now let $\mathfrak{a}_0$ be as in § 5.2 and consider the adjoint representation of $\mathfrak{a}_0$ on $\mathfrak{g}$. It follows immediately from § 2.5(d) and (5.3.4) that (1) e_ψ lies in an irreducible component $\mathfrak{b} \subseteq \mathfrak{g}$, (2) $\dim \mathfrak{b} = 2q+1$, (3) $e_{-\psi} \in \mathfrak{b}$ and (4) any other irreducible has dimension less than $\dim \mathfrak{b}$. A direct consequence of these facts is that

$$(\operatorname{ad} e_0)^{2q+1} = 0$$

and

$$(\operatorname{ad} e_0)^{2q}(e_{-\psi}) = a e_\psi$$

where $a \neq 0$.

Now since e is conjugate to e_0 it follows that $(\operatorname{ad} e)^{2q} \neq 0$. On the other hand, since $e \in \mathfrak{n}$, it follows that for any $\phi \in \Delta$ we can write

$$(\operatorname{ad} e)^{2q}(e_\phi) = \sum_{\xi \in \Delta} b_\xi e_\xi \tag{5.3.6}$$

and, moreover, $b_\xi \neq 0$ implies

$$o(\xi) \geqq o(\phi) + 2q.$$

But this together with (5.3.4) implies that (5.3.6) vanishes for all $\phi \neq -\psi$. Thus $(\operatorname{ad} e)^{2q}(e_{-\psi}) \neq 0$ and in fact, using (5.3.4) once more,

$$(\operatorname{ad} e)^{2q} e_{-\psi} = a' e_\psi$$

for some non-zero scalar a'. Now write $e = e_1 + e_2$, where $e_1 \in \mathfrak{g}_1$ and $e_2 \in \mathfrak{n}_2$.

Expanding $(\operatorname{ad} e)^{2q} = (\operatorname{ad} e_1 + \operatorname{ad} e_2)^{2q}$ it is clear again from (5.3.4) that

$$(\operatorname{ad} e)^{2q}(e_{-\psi}) = (\operatorname{ad} e_1)^{2q}(e_{-\psi}) = a' e_\psi.$$

But for any i, writing

$$(\operatorname{ad} e_1)^{i}(e_{-\psi}) = \sum_{\xi \in \Delta} b'_\xi e_\xi,$$

it follows that since $a_{\alpha_j} = 0$, one can have $b'_\xi \neq 0$ only when upon writing

$$\xi = \sum_{i=1}^{l} t_i \alpha_i,$$

we have $t_j = -q_j$. In particular, setting $i = 2q$ this means $q_j = -q_j$ or $q_j = 0$. This contradicts (5.3.3) and hence Theorem 5.3 is proved when $\mathfrak{g}$ is simple. The general case follows immediately upon writing $\mathfrak{g}$ as a direct sum of its simple ideals. The component of e in each ideal is necessarily principal nilpotent in that ideal by Corollary 5.3. Q. E. D.

5.4. A theorem proved in [1] (See [1], Remark p. 66.) asserts that every solvable subalgebra $\mathfrak{s}_1$ of $\mathfrak{g}$ is conjugate to a subalgebra $\mathfrak{s}'_1$ of $\mathfrak{s}$. If in addition it is assumed that the elements of $\mathfrak{s}_1$ are all nilpotent (hence $\mathfrak{s}_1$ is a nilpotent Lie algebra by Engel's theorem), it is clear then that $\mathfrak{s}'_1 \subseteq \mathfrak{n}$. In particuar, it follows then that every nilpotent element $e \in \mathfrak{g}$ is conjugate to some element $e' \in \mathfrak{n}$. Actually, we don't need the result of [1] referred to above to prove this. For completeness, we observe that this follows from Lemma 5.1.

LEMMA 5.4. *Any nilpotent element $e \in \mathfrak{g}$ is conjugate to an element $e' \in \mathfrak{n}$.*

Proof. Applying Theorem 3.4 it suffices only to show that the nilpositive element of any S-triple containing x_j (using the notation of Lemma 5.1) as neutral element lies in $\mathfrak{n}$. But this is clear since $x_j \in D$. That is, for $\phi \in \Delta$, $(x_j, \phi) = 1$ implies $\phi \in \Delta^+$.

As a corollary to Theorem 5.3, its proof, and Lemma 5.4 we obtain another characterization of principal nilpotent elements in case $\mathfrak{g}$ is simple.

COROLLARY 5.4. *Assume $\mathfrak{g}$ is simple. Let ψ be the highest root and let $q = o(\psi)$. Let $e \in \mathfrak{g}$ be any nilpotent element. Then e is principal nilpotent if and only if $(\operatorname{ad} e)^{2q} \neq 0$. However, if e is principal nilpotent $(\operatorname{ad} e)^{q+1} = 0$.*

5.5. Corollary 3.7 sets up a natural one-one relation between the conjugate classes of nilpotent elements and the conjugate classes of TDS. It is clear that in this correspondence the class of principal nilpotent elements corresponds to the class of principal TDS. Regarding the latter as distinctive among all conjugate classes of TDS will be given further justification then when it is shown that the former is distinctive among conjugate classes of nilpotent elements. The following corollary shows this very clearly.

COROLLARY 5.5. *The set of principal nilpotent elements (a conjugate class of the adjoint group G) in $\mathfrak{g}$ forms an open, dense and connected subset of the set of all nilpotent elements in $\mathfrak{g}$.*

Proof. Openness follows easily from Corollary 5.3 by choosing a basis

of $\mathfrak{g}$ and considering the $(n-l)\times(n-l)$ minors of the matrix defined by $\operatorname{ad} e$, e nilpotent, with respect to the basis. Denseness follows from Theorem 5. 3 and Lemma 5. 4. Connectivity is immediate also since the set of principal nilpotent elements is an orbit of the group G.

5. 6. Principal nilpotent elements behave like the "regular" elements in the set of all nilpotent elements. That is, one can make a strong case for the following analogy: The set of principal nilpotent elements is to the set of all nilpotent elements as the set of all regular elements is to the set of all semi-simple elements. We cite for example Corollary 5. 3 and Corollary 5. 5. In this analogy, between the semi-simple elements and the nilpotent elements, the Cartan subalgebra clearly corresponds to the maximum Lie subalgebra of nilpotent elements (see Lemma 5. 4 § 2. 1. Also all maximum Lie subalgebras of nilpotent elements are conjugate—see § 5. 4). One knows that a regular element can be characterized by the property that it lies in one and only one Cartan subalgebra. Corollary 5. 6 asserts that also in this regard the analogy still holds.

COROLLARY 5. 6. *Let $e\in\mathfrak{g}$ be nilpotent. (One knows that e can be embedded in at least one maximal Lie subalgebra of nilpotent elements.) Then e is principal nilpotent if and only if e lies in one and only one maximal Lie subalgebra of nilpotent elements of $\mathfrak{g}$.*

Proof. By Lemma 5. 4 we may assume $e\in\mathfrak{n}$ (using the notation § 5. 4). Assume that e is not principal. We will prove e is contained in a second (different) maximal Lie subalgebra of nilpotent elements $\mathfrak{n}'$. Now we may write

$$e=\sum_{\phi\in\Delta^+} a_\phi e_\phi.$$

By Theorem 5. 3 since e is not principal, $a_{\alpha_i}=0$ for some value of i. But now it is known (and easy to verify) that

$$\mathfrak{n}'=\sum_{\substack{\phi\in\Delta^+\\ \phi\neq\alpha_i}}(e_\phi)+(e_{-\alpha_i})$$

is a maximal Lie subalgebra of nilpotent elements of $\mathfrak{g}$. (In fact, $\mathfrak{n}$ is carried onto $\mathfrak{n}'$ by any element of G which (1) leaves $\mathfrak{h}$ invariant and (2) whose restriction to $\mathfrak{h}$ is the reflection R_{α_i}—see § 7. 1). Obviously $e\in\mathfrak{n}'$.

Now assume e is principal. In fact, we may take $e=e_0$, where we use the notation of § 5. 2. Assume $e_0\in\mathfrak{n}'$, where $\mathfrak{n}'=A\mathfrak{n}$, $A\in G$. We shall use

the prime ($'$) on previous notation to indicate the effect of conjugation by A. Applying Theorem 5.3 to $\mathfrak{n}'$ it follows that

$$e_0 = \sum_{\phi \in \Delta^+} a_\phi e_\phi',$$

where $a_\phi \neq 0$ for $\phi = \alpha_i$, $i = 1, 2, \cdots, l$. Now by Theorem 4.3 there exists $A_1 \in N'$ such that

$$A_1 e_0 = \sum_{i=1}^{l} a_{\alpha_i} e_{\alpha_i}'.$$

But then since x_0' $(= Ax\ )$ and $A_1 e_0$ are clearly the neutral and nil-postive elements of an S-triple (see proof of Lemma 5.2), it follows from Theorem 3.6 that

$$A_1 x_0 \in x_0' + \mathfrak{g}^{A_1 e_0}.$$

However, since x_0' is regular upon applying § 2.5(d) and (5.1.2) in the case of this S-triple, it follows that $\mathfrak{g}^{A_1 e_0} \subseteq \mathfrak{n}'$. But then by Theorem 4.3 there exists $A_2 \in N'$ such that $A_2 A_1 x_0 = x'_0$. But now since x_0 is regular, we must have $A_2 A_1 \mathfrak{h} = \mathfrak{h}'$. But this of course implies $\mathfrak{h} \subseteq \mathfrak{s}'$ because $A_1^{-1} A_2^{-1} \in S'$. But this means $\mathfrak{s}'$ and hence $\mathfrak{n}' = [\mathfrak{s}', \mathfrak{s}']$ are stable under ad $\mathfrak{h}$. But then $\mathfrak{n}'$ must contain and in fact must be spanned by root vectors associated with $\mathfrak{h}$ (since obviously $\mathfrak{n}' \cap \mathfrak{h} = 0$). But $e_0 = \sum_{i=1}^{l} c_i e_{\alpha_i} \in \mathfrak{n}'$ and $c_i \neq 0$. Thus $e_{\alpha_i} \in \mathfrak{n}'$, $i = 1, 2, \cdots, l$. Hence since the e_{α_i} generate $\mathfrak{n}$, it follows that $\mathfrak{n} \subseteq \mathfrak{n}'$. But then of course $\mathfrak{n} = \mathfrak{n}'$. Q. E. D.

5.7. We continue with previous notation.

Now consider $\mathfrak{g}^{e_0}$, the kernel of ad e_0. By Corollary 5.3

$$\dim \mathfrak{g}^{e_0} = l.$$

In the special case when $\mathfrak{g}$ is the set of all $(l+1) \times (l+1)$ complex matrices of trace zero one sees easily that $\mathfrak{g}^{e_0}$ is a commutative Lie algebra (of nilpotent matrices). This and other evidence suggested to us that perhaps $\mathfrak{g}^{e_0}$ is commutative in the general case. However, since among other things we were unable to construct a "useable" basis of $\mathfrak{g}^{e_0}$ we could not settle the question using purely algebraic methods. Nevertheless, it is true that $\mathfrak{g}^{e_0}$ is commutative (Corollary 5.8) in the general case. The proof which we have found is very simple but uses limit arguments. It was Corollary 5.8 which orignally suggested the validity of Theorem 6.7.

Theorem 5.7 or Corollary 5.7 may be regarded as a generalization of the fact that a Cartan subalgebra of a semi-simple Lie algebra is commutative.

THEOREM 5.7. *Let* $\mathfrak{g}$ *be a complex semi-simple Lie algebra of rank* l. *Let* $y \in \mathfrak{g}$ *be arbitrary. Then* $\mathfrak{g}^y$ *contains an* l *dimensional commutative Lie subalgebra.*

Proof. It is well known that the set of regular elements in $\mathfrak{g}$ is dense in $\mathfrak{g}$. Thus we may find a sequence y'_n, $n = 1, 2, \cdots$ of regular elements converging to y.

Now consider the Grassmann manifold of all l planes in $\mathfrak{g}$. This, of course, is compact and hence we may find a subsequence y_n of the sequence y'_n with the property $y_n \to y$ and the Cartan subalgebras $\mathfrak{g}^{y_n}$ converge to an l-plane $\mathfrak{u}$ in the Grassmann manifold. Now if w_i, $i = 1, 2, \cdots, l$, is any basis of $\mathfrak{u}$ we may find elements $w_i^n \in \mathfrak{g}$, $n = 1, 2, \cdots$, $i = 1, 2, \cdots, l$, such that $w_i^n \in \mathfrak{g}^{y_n}$ and $w_i^n \to w_i$ as $n \to \infty$ for $i = 1, 2, \cdots, l$. Since $[y_n, w_i^n] = 0$, it follows immediately by taking the limit that $\mathfrak{u} \subseteq \mathfrak{g}^y$. But $[w_i^n, w_j^n] = 0$. Again taking the limit this obviously implies $\mathfrak{u}$ is commutative. Q. E. D.

COROLLARY 5.7. *Let* $y \in \mathfrak{g}$. *Assume* $\dim \mathfrak{g}^y = 1$. *Then* $\mathfrak{g}^y$ *is commutative.*

5.8. Corollary 5.7 and Corollary 5.3 imply

COROLLARY 5.8. *Let* e *be a principal nilpotent element in* $\mathfrak{g}$. *Then* $\mathfrak{g}^e$ *is commutative.*

6. The principal element of G and the duality theorem.

1. We shall assume from now on that $\mathfrak{g}$ is simple. The theorems to be proved are either true in the general semi-simple case or can be obviously modified to be true in that case. The extension from the simple case to the semi-simple case in any event is immediate. We consider only the former mainly for notational simplicity.

Recall what is meant by a compact form $\mathfrak{k}$ of $\mathfrak{g}$. This may be defined as a real Lie subalgebra of $\mathfrak{g}$ with the property

$$\mathfrak{g} = \mathfrak{k} + i\mathfrak{k} \tag{1}$$

is a real direct sum. (That is, $\mathfrak{k}$ is just a "real form" of $\mathfrak{g}$ and

(2) The restriction of B to $\mathfrak{k}$ is negative definite.

One immediate consequence of (2) is

(a) every element of $\mathfrak{k}$ is semi-simple. Next we recall some facts in the Cartan subalgebra theory of $\mathfrak{k}$ (which is somewhat different from that of $\mathfrak{g}$).

(b) If $\mathfrak{t}$ is a Cartan subalgebra of $\mathfrak{k}$, then $\mathfrak{h}_1 = \mathfrak{t} + i\mathfrak{t}$ is a Cartan subalgebra of $\mathfrak{g}$ and $\mathfrak{h}_1{}^{\#} = i\mathfrak{t}$.

(c) A Lie subalgebra $\mathfrak{t}$ of $\mathfrak{k}$ is a Cartan subalgebra if and only if it is maximal commutative.

An immediate consequence of (c) which we shall soon use is

(d) Any commutative Lie subalgebra $\mathfrak{u}$ of $\mathfrak{k}$ can be imbedded in a Cartan subalgebra of $\mathfrak{k}$.

Corresponding to the adjoint operation (conjugate transpose) in the space of matrices we introduce a *-operation in $\mathfrak{g}$ by defining for any $z \in \mathfrak{g}$

$$z^* = x - iy,$$

where z is written

$$z = x + iy$$

for $x, y \in i\mathfrak{k}$.

Generalizing the notion of a normal matrix or normal operator we will say $z \in \mathfrak{g}'$ is normal with respect to $\mathfrak{k}$ whenever

$$[z, z^*] = 0$$

Writing $z = x + iy$, $x, y \in i\mathfrak{k}$ it is clear that z is normal if and only if $[x, y] = 0$.

It is well known of course that a normal matrix is diagonizable (semi-simple). The following generalization of this fact (and also of (a)) is a useful criterion for semi-simplicity in $\mathfrak{g}$.

LEMMA 6.1. *Let z, an element of $\mathfrak{g}$, be normal with respect to a compact form $\mathfrak{k}$ of $\mathfrak{g}$. Then z is a semi-simple element of $\mathfrak{g}$.*

Proof. We may write $z = x + iy$, where $ix, iy \in \mathfrak{k}$. But now since z is normal $[ix, iy] = 0$. Thus by (d) there exists a Cartan subalgebra $\mathfrak{t}$ of $\mathfrak{k}$ which contains ix and iy. But by (b) $\mathfrak{h}_1 = \mathfrak{t} + i\mathfrak{t}$ is a Cartan subalgebra of $\mathfrak{g}$. But then $z \in \mathfrak{h}_1$ and hence z is semi-simple. Q. E. D.

When the root vectors, relative to a Cartan subalgebra, are suitably normalized (Weyl's normal form) Weyl has given a basis of a compact form of $\mathfrak{g}$ in terms of these root vectors and the Cartan subalgebra. In previous sections we required no other normalization of the e_ϕ, $\phi \in \Delta$, other than (5.1.0). We will assume from here on, unless specified otherwise (in Theorem 8.4), that the root vectors are normalized into Weyl's normal form, with the exception that $(e_\phi, e_{-\phi}) = 1$ is retained in preference to $(e_\phi, e_{-\phi}) = -1$. (In such a normal form one may choose the root vectors e_{α_i},

$i = 1, 2, \cdots, l$, arbitrarily and hence we need not regard e_0 as having been altered). Then one knows that the linear span, with real coefficients, of $i\mathfrak{h}^{\#}$ and the vectors $e_\phi - e_{-\phi}$, $ie_\phi + ie_{-\phi}$ for all $\phi \in \Delta^+$ is a compact form $\mathfrak{k}$ of $\mathfrak{g}$. (See remark, p. 11-11 in [12]). One sees easily then that $(e_\phi)^* = e_{-\phi}$ or

$$(6.1.1) \qquad (\sum_{\phi \in \Delta} a_\phi e_\phi)^* = \sum_{\phi \in \Delta} \bar{a}_\phi e_{-\phi}$$

for any set of complex numbers a_ϕ, $\phi \in \Delta$.

6.2. We recall now (see § 6.1) that $\mathfrak{g}$ is simple. Let $\psi \in \Delta$ be the highest root.[8] Let $\Pi^Q \subseteq \Delta$ be the subset of $l+1$ roots obtained by adjoining $-\psi$ to the simple positive roots. That is, $\Pi^Q = \Pi \cup (-\psi)$. The notion of simple root and highest root are notions which of course are relative to the choice of a lexicographical ordering in $\mathfrak{h}^{\#}$ or rather to the choice of a Weyl chamber (see § 5.1). We will say then that the roots in Π^Q are Q-simple relative to the chamber D. (We shall not require the fact but it can be shown that the number of Weyl chambers which give rise to the same set of Q-simple roots is equal to order of the fundamental group of G; that is, to the order of the center of the simply connected covering group of G.)

Now an element $z \in \mathfrak{g}$ will be called cyclic if there exists a Cartan subalgebra $\mathfrak{h}_1$ and a set $\Pi_1{}^Q \subseteq \Delta_1$ of Q-simple roots relative to some Weyl chamber D_1 in $\mathfrak{h}_1{}^{\#}$ such that z can be written

$$(6.2.1) \qquad z = \sum_{\xi \in \Pi_1{}^Q} a_\xi e_\xi,$$

where the a_ξ, $\xi \in \Pi_1{}^Q$, are non-zero complex numbers and the e_ξ are root vectors for $\mathfrak{h}_1$ corresponding to the roots $\xi \in \Delta_1$.[9] Cyclic elements play a major role in the remainder of this paper.

If z is given by (6.2.1), observe that in effect we have formed the cyclic element z by adding $a_{-\psi_1} e_{-\psi_1}$ to a principal nilpotent element, where ψ_1 is the highest root in Δ_1 relative to D_1. It shall be shown that not only does this destroy nilpotency but the cyclic elements are in fact regular. First we shall need

LEMMA 6.2. *Let the cyclic elements $z, z' \in \mathfrak{g}$ be given by*

$$z = \sum_{\beta \in \Pi^Q} a_\beta e_\beta$$

and

$$z' = \sum_{\beta \in \Pi^Q} a'_\beta e_\beta,$$

[8] The properties of ψ which will be required are all consequences of (5.3.5).

[9] The set Δ_1 is the set of roots associated with the Cartan subalgebra $\mathfrak{h}_1$.

where the coefficients a_β, a'_β are all arbitrary non-zero complex numbers. Then if H is the subgroup of G corresponding to $\mathfrak{h}$ there exists an element $A \in H$ and a non-zero scalar λ such that

$$Az = \lambda z'.$$

Proof. Let ϵ_i, $i = 1, 2, \cdots, l$, be as in § 5.1. Let $y \in \mathfrak{h}$ be given by

$$y = \sum_{i=1}^{l} \operatorname{Log}(a'_{\alpha_i}/a_{\alpha_i})\epsilon_i.$$

Clearly $\operatorname{Exp} y \in H$ and

$$\operatorname{Exp} y\left(\sum_{i=1}^{l} a_{\alpha_i} e_{\alpha_i}\right) = \sum_{i=1}^{l} a'_{\alpha_i} e_{\alpha_i}.$$

Now let c be any complex number and let x_0 be given by (5.2.1). Then clearly

$$\operatorname{Exp}(y + cx_0)\left(\sum_{i=1}^{l} a_{\alpha_i} e_{\alpha_i}\right) = e^c\left(\sum_{i=1}^{l} a'_{\alpha_i} e_{\alpha_i}\right). \tag{6.2.1}$$

Now let $q = o(\psi)$ as in § 5.3. But then

$$\operatorname{Exp} cx_0(e_{-\psi}) = e^{-cq} e_{-\psi}$$

and if b is defined by $\operatorname{Exp} y(e_{-\psi}) = be_{-\psi}$, then $b \neq 0$ and

$$\operatorname{Exp}(y + cx_0)(a_{-\psi} e_{-\psi}) = e^{-cq} b a_{-\psi} e_{-\psi}. \tag{6.2.2}$$

Now choose c so that

$$e^{-c(q+1)} = a'_{-\psi}/ba_{-\psi}.$$

Then

$$e^{-cq} b a_{-\psi} = e^c a'_{-\psi}. \tag{6.2.3}$$

Hence if $\lambda = e^c$, $A = \operatorname{Exp}(y + cx_0)$, one has $A \in H$ and (6.2.1), (6.2.2), and (6.2.3) imply

$$A\left(\sum_{\beta \in \Pi^0} a_\beta e_\beta\right) = \lambda\left(\sum_{\beta \in \Pi^0} a'_\beta e_\beta\right). \qquad \text{Q.E.D.}$$

An immediate consequence of Lemma 6.2 is the following theorem which asserts that up to scalar multiplication the set of cyclic elements forms a single conjugate class in $\mathfrak{g}$.

THEOREM 6.2. *Let z and z' be any two cyclic elements in $\mathfrak{g}$. Then there exists a scalar λ, $\lambda \neq 0$, such that z and $\lambda z'$ are conjugate to each other.*

Proof. If D_1 is a Weyl chamber in $\mathfrak{h}_1{}^\#$, where $\mathfrak{h}_1$ is a Cartan subalgebra, there exists $A \in G$ such that $A\mathfrak{h}_1 = \mathfrak{h}_1$ and $AD_1 = D$. This fact together with Lemma 6.2 proves Theorem 6.2. Q.E.D.

6.3. Lemma 6.1 is needed solely to prove the following lemma.

LEMMA 6.3. *Cyclic elements are semi-simple.*

Proof. Now if we write

$$\psi = \sum_{i=1}^{l} q_i \alpha_i, \tag{6.3.1}$$

recall that the coefficients q_i are positive integers. (See (5.3.3)). Thus if e_1 is defined by

$$e_1 = \sum_{i=1}^{l} (q_i)^{\frac{1}{2}} e_{\alpha_i}$$

and z_1 is defined by

$$z_1 = e_1 + e_{-\psi},$$

then e_1 and z_1 are, respectively, principal nilpotent and cyclic elements.

To prove Lemma 6.3 it suffices by Theorem 6.2 to prove only that z_1 is semi-simple. But to prove that z_1 is semi-simple, by Lemma 6.1 it suffices only to prove that z_1 is normal with respect to $\mathfrak{k}$. Now by (6.1.1)

$$z_1{}^* = e_1{}^* + e_\psi$$

and

$$e_1{}^* = \sum_{i=1}^{l} (q_i)^{\frac{1}{2}} e_{-\alpha_i}.$$

But, obviously then, since ψ is the highest root

$$[e_1, e_\psi] = [e_1{}^*, e_{-\psi}] = 0.$$

Thus

$$[z_1, z_1{}^*] = [e_1 + e_{-\psi}, e_1{}^* + e_\psi] = [e_1, e_1{}^*] + [e_{-\psi}, e_\psi].$$

But

$$[e_1, e_1{}^*] = \sum_{i=1}^{l} q_i [e_{\alpha_i}, e_{-\alpha_i}] = \sum_{i=1}^{l} q_i \alpha_i = \psi$$

by (5.1.1) and (6.3.1). On the other hand, of course,

$$[e_{-\psi}, e_\psi] = -\psi.$$

Thus $[z_1, z_1{}^*] = 0$ and hence z_1 is normal with respect to $\mathfrak{k}$. Q.E.D.

6.4. To gain information on cyclic elements in general it suffices by Theorem 6.2 to focus attention on a single fixed cyclic element. We choose this element to be z_0, where z_0 is given by

$$z_0 = e_0 + e_{-\psi}. \tag{6.4.1}$$

Here, of course, e_0 is given by (5.2.2).

As in § 5.2 let $\mathfrak{a}_0$ be the TDS spanned by x_0, e_0 and f_0. Now let n_k be the multiplicity of the irreducible $2k+1$-dimensional representation π_{2k+1} in the complete reduction of the adjoint representation of $\mathfrak{a}_0$ on $\mathfrak{g}_0$. By Corollary 5.2, $n_k = 0$ if k is a half-integer and

$$l = n_0 + n_1 + n_2 + \cdots. \tag{6.4.2}$$

Now it follows from § 2.5(d) and (5.2.4) that the kernel $\mathfrak{g}^{e_0}$ of $\operatorname{ad} e_0$ is contained in $\mathfrak{s}$. On the other hand, it is obvious that $\mathfrak{g}^{e_0} \cap \mathfrak{h} = 0$. Therefore, since $x_0 \in \mathfrak{h}$ is regular, it follows that the eigenvalues of $\operatorname{ad} x_0$ on $\mathfrak{g}^{e_0}$ are positive. This implies two things, (1) $\mathfrak{g}^{e_0} \subseteq \mathfrak{n}$ (Actually, we have already noted this fact—see proof of Corollary 5.6) and (2) by § 2.5(d), $n_0 = 0$. That is, only the zero element is annihilated by $\operatorname{ad} \mathfrak{a}_0$. Indeed, this also follows from § 2.5(h) which asserts

$$\begin{aligned} n_0 &= \dim \mathfrak{g}_0 - \dim \mathfrak{g}_1 \\ &= l - l \\ &= 0. \end{aligned}$$

For the present we direct our attention to the first fact, $\mathfrak{g}^{e_0} \subseteq \mathfrak{n}$.

Let $\mathfrak{n}^*$ be the maximal Lie subalgebra of nilpotent elements given by

$$\mathfrak{n}^* = \sum_{\phi \in \Delta^+} (e_{-\phi}).$$

Then, of course,

$$\mathfrak{g} = \mathfrak{n}^* + \mathfrak{h} + \mathfrak{n} \tag{6.4.3}$$

is a direct sum decomposition. We shall let ρ (resp. ρ^*) be the projection

$$\rho : \mathfrak{g} \to \mathfrak{n}$$
$$(\text{resp. } \rho^* : \mathfrak{g} \to \mathfrak{n}^*)$$

of $\mathfrak{g}$ onto $\mathfrak{n}$ (resp. $\mathfrak{n}^*$) defined by the decomposition (6.4.3).

Now consider the kernel $\mathfrak{g}^{z_0}$ of $\operatorname{ad} z_0$. A relation between $\mathfrak{g}^{e_0}$ and $\mathfrak{g}^{z_0}$ is given by

LEMMA 6.4A. *Let ρ_0 be the restriction of the projection to the subspace $\mathfrak{g}^{z_0}$. Then $\rho_0(\mathfrak{g}^{z_0}) \subseteq \mathfrak{g}^{e_0}$ and in fact*

$$\rho_0 : \mathfrak{g}^{z_0} \to \mathfrak{g}^{e_0}$$

is a linear isomorphism of $\mathfrak{g}^{z_0}$ onto $\mathfrak{g}^{e_0}$.

Proof. It follows immediately from the decomposition (6.4.3) of $\mathfrak{g}$ and (5.1.3) that

$$[e_{-\psi}, \mathfrak{n}] \subseteq \mathfrak{n}^* + \mathfrak{h}$$
$$[e_{-\psi}, \mathfrak{h}] \subseteq (e_{-\psi})$$
$$[e_{-\psi}, \mathfrak{n}^*] = 0.$$

Now let $y \in \mathfrak{g}^{z_0}$ be arbitrary. Write

$$y = v + x + u,$$

where $v \in \mathfrak{n}^*$, $x \in \mathfrak{h}$, and $u \in \mathfrak{n}$.

Now by (6.4.1) and § 5.1

$$\begin{aligned} 0 &= [z_0, y] \\ &= [e_0, v] + [e_0, x] + [e_0, u] \\ &\quad + (x, \psi) e_{-\psi} + [e_{-\psi}, u]. \end{aligned} \tag{6.4.4}$$

Applying the projection ρ to both sides of (6.4.4) we obtain

$$[e_0, x] + [e_0, u] = 0.$$

But then recalling the relation $[\mathfrak{g}_i, \mathfrak{g}_j] \subseteq \mathfrak{g}_{i+j}$, it is clear that $[e_0, x] = 0$ and $[e_0, u] = 0$. Thus since $u = \rho(y)$ it follows that $\rho(\mathfrak{g}^{z_0}) \subseteq \mathfrak{g}^{e_0}$. It also follows that since $\mathfrak{g}^{e_0} \subseteq \mathfrak{n}$, we must have

$$x = 0. \tag{6.4.5}$$

Thus $y = v + u$ and

$$0 = [e_0, v] + [e_0, u] + [e_{-\psi}, u].$$

To show first that ρ_0 is one-one, assume $u = 0$. But this and the last expression imply that $v \in \mathfrak{g}^{e_0}$. But $\mathfrak{g}^{e_0} \subseteq \mathfrak{n}$. Hence $v = 0$. Thus $y = 0$ which proves that ρ_0 is an isomorphism into. But now, by Corollary 5.3, $\dim \mathfrak{g}^{e_0} = l$. On the other hand, $\dim \mathfrak{g}^{z_0} \geqq l$ (see, for example Theorem 5.7). Since ρ_0 is an isomorphism, this means

$$\dim \mathfrak{g}^{z_0} = l$$

and also that ρ_0 is onto. Q. E. D.

A major consequence of Lemma 6.4A is

COROLLARY 6.4. *Cyclic elements are regular.*

Proof. As above let z_0 be defined by (6.4.1). It suffices to show z_0 is regular. But by Lemma 6.3 z_0 is semi-simple. Hence $\mathfrak{g}^{z_0}$ contains a Cartan subalgebra. But, by Lemma 6.4, $\dim \mathfrak{g}^{z_0} = l$. Hence z_0 is regular.

Corollary 6.4 implies

LEMMA 6.4B. *Let* z_0 *be defined by* (6.4.1). *Then* $\mathfrak{g}^{z_0}$ *is a Cartan subalgebra.*

We will let $\mathfrak{h}'$ designate the Cartan subalgebra $\mathfrak{g}^{z_0}$.

In the proof of Lemma 6.4 we considered the decomposition of any element $y \in \mathfrak{h}'$ and showed that its projection x in $\mathfrak{h}$ vanishes. (See (6.4.5)). We state this as

LEMMA 6.4C. *Let* z_0 *be defined by* (6.4.1). *Let* ρ *and* ρ^* *be the projections of* $\mathfrak{g}$ *on* $\mathfrak{n}$ *and* $\mathfrak{n}^*$ *also defined as in* § 6.4. *Then the projection* $1-(\rho+\rho^*)$ *of* $\mathfrak{g}$ *on* $\mathfrak{h}$ *vanishes on* $\mathfrak{h}'$.

Perhaps a simpler way of expressing Lemma 6.4C is to state that the Cartan subalgebras $\mathfrak{h}'$ and $\mathfrak{h}$ are orthogonal to each other (with respect to B).

6.5. Now $\mathfrak{g}^{e_0}$ is invariant under $\operatorname{ad} x_0$ (see § 2.5(d)). Let u_i, $i=1,2,\cdots,l$, be a basis of $\mathfrak{g}^{e_0}$ and also eigenvectors of $\operatorname{ad} x_0$. Let k_i, $i=1,2,\cdots,l$, be the corresponding eigenvalues. That is, $u_i \in \mathfrak{g}_{k_i}$, $i=1,2,\cdots,l$. We may regard the basis so ordered that $k_i \leqq k_{i+1}$. At this stage we already know two of the k_i, namely, the extreme ones k_1 and k_l. We also know an inequality, $k_{l-1} < k_l$.

LEMMA 6.5A. *Let* k_i *be defined as above. Then, where* $q = o(\psi)$,

$$1 = k_1 \leqq k_i \leqq \cdots \leqq k_{l-1} < k_l = q.$$

Proof. As we noted in § 6.4 we must have $k_1 > 0$. On the other hand, since $e_0 \in \mathfrak{g}^{e_0}$, it follows that $k_1 = 1$. But also $e_\psi \in \mathfrak{g}^{e_0}$ since ψ is the highest root. Thus $[x_0, e_\psi] = q e_\psi$ implies $k = q$. Since $o(\phi) < q$ for every $\phi \neq \psi$ (see (5.3.4)), it also follows that $k_{l-1} < k_l$. Q.E.D.

Taking the proof of Lemma 6.5A into account we will choose $u_1 = e_0$ and $u_l = e_\psi$.

Now let d_i, $i=1,2,\cdots,l$, be the dimensions, in non-decreasing order, of the irreducible components occurring in the complete reduction of adjoint representation of a principal TDS (e.g. $\mathfrak{a}_0$) on $\mathfrak{g}$. Appplying § 2.5(d) the eigenvalues k_i yield the dimensions d_i by the relation

$$d_i = 2k_i + 1. \tag{6.5.1}$$

Lemma 6.5A implies $d_1 = 3$, $d_l = 2q+1$ and $d_{l-1} < 2q+1$.

Now by Lemma 6.4A there exists a unique basis $y_1, y_2, \cdots, y_l$ of the Cartan subalgebra $\mathfrak{h}'$ with the property that $\rho(y_i) = u_i$. Define v_i by

$$y_i = u_i + v_i. \tag{6.5.2}$$

By Lemma 6.4C it follows that $v_i \in \mathfrak{n}^*$ for $i=1,2,\cdots,l$. Since $u_1 = e_0$ and since $\rho(z_0) = e_0$, it follows from (6.4.1) and Lemma 6.4A that $v_1 = e_{-\psi}$ and $y_1 = z_0$. Now $u_l = e_\psi$. We shall have to know what v_l is.

LEMMA 6.5B. *Let c_i and q_i, $i=1,2,\cdots,l$, be defined respectively by* (5.2.2) *and* (6.3.1). *Then v_l is the element given by*

$$v_l = \sum_{i=1}^{l} (q_i/c_i) e_{-\alpha_i}. \tag{6.5.3}$$

Proof. As in the proof of Lemma 6.3

$$\begin{aligned}[z_0, e_\psi + \sum_{i=1}^{l} (q_i/c_i) e_{-\alpha_i}] \\ &= [e_{-\psi}, e_\psi] + \sum_{i=1}^{l} q_i [e_{\alpha_i}, e_{-\alpha_i}] \\ &= -\psi + \sum_{i=1}^{l} q_i \alpha_i = 0.\end{aligned}$$

Thus $e_\psi + \sum_{i=1}^{l} (q_i/c_i) e_{-\alpha_i} \in \mathfrak{h}'$. It follows immediately then from Lemma 6.4A that $v_l = \sum_{i=1}^{l} (q_i/c_i) e_{-\alpha_i}$. Q.E.D.

6.6. Now it is clear (for example from the matrix representation of a TDS given in §2.5) that there exists an element A in the subgroup of G corresponding to $\mathfrak{a}_0$ such that $Ax_0 = -x_0$. But since x_0 is regular, it is clear then that

$$A : \mathfrak{h} \to \mathfrak{h},$$
$$A : \mathfrak{n}^* \to \mathfrak{n}.$$

In fact these relations are already contained in the more general fact

$$A : \mathfrak{g}_j \to \mathfrak{g}_{-j}$$

for any $-q \leqq j \leqq q$. It follows then that we may interchange the roles of Δ^+ and $-\Delta^+$, $\mathfrak{n}$ and $\mathfrak{n}^*$ and also $\mathfrak{g}_1$ and $\mathfrak{g}_{-1}$ in the results of §§6.2-5. But then one sees that v_l is principal nilpotent and that $y_l = u_l + v_l$ is cyclic. But then by Corollary 6.4 it follows that $\mathfrak{g}^{v_l} = \mathfrak{h}'$. Finally, applying Lemma 6.4A we obtain

LEMMA 6.6. *We retain previous notation. Let ρ^*_0 be the restriction of ρ^* to $\mathfrak{h}'$. Then (1) v_l is a principal nilpotent element, (2), $\rho^*_0(\mathfrak{h}') \subseteq \mathfrak{g}^{v_l}$ and in fact*

$$\rho^*_0 : \mathfrak{h}' \to \mathfrak{g}^{v_l}$$

is isomorphism onto. In other words, the elements v_i, $i=1,2,\cdots,l$, *form a basis of* $\mathfrak{g}^{v_l}$. *Also, the elements* v_i *commute with each other.* (*See Corollary* 5.8).

It is obvious from (5.2.3) that v_l is a nil-negative element of a principal S-triple containing x_0 as neutral element or an nil-positive element of a principal S-triple containing $-x_0$ as neutral element. Thus $\mathfrak{g}^{v_l}$ is stable under $\operatorname{ad} x_0$ and since all principal S-triples are conjugate the eigenvalues of $\operatorname{ad} x_0$ on $\mathfrak{g}^{v_l}$ are $-k_l, -k_{l-1},\cdots,-k_1$ in non-decreasing order. The elements v_i are a basis of $\mathfrak{g}^{v_l}$ by Lemma 6.6 but it is not at all clear yet that they are eigenvectors of $\operatorname{ad} x_0$.

6.7. We now isolate a particular conjugate class in G, elements of which, will play a major role in the remainder of this paper. An element $P\in G$ will be called a principal element of G if there exists a principal regular element $x\in\mathfrak{g}$ (see § 5.2) such that P can be written

$$P=\operatorname{Exp}(2\pi i/s)x, \tag{6.7.1}$$

where $s=q+1$ and q, as usual, is the order of the highest root ψ. Note that since x lies in a principal TDS, the principal element P lies in a subgroup of G corresponding to a principal TDS. (We shall make no use of the fact here but it can be shown that the number of principal regular elements x which satisfy (6.7.1) for a fixed principal element $P\in G$ is equal to order of the fundamental group of G). Various characterizations of principal elements will be given in §§ 8 and 9.

Throughout the remainder of the paper we will let ω be the primitive s root of unity defined by $\omega=e^{2\pi i/s}$. Let P_0 be principle element in G defined by letting $P_0=\exp(2\pi i/s)x_0$. It is clear then that

$$P_0u=\omega^j u$$

for $u\in\mathfrak{g}_j$, $-q\leqq j\leqq q$. It follows then that ω^j, $j=0,1,\cdots,q$, are the eigenvalues of P_0 and if $\mathfrak{u}_j$ designates the corresponding eigenspaces, then

$$\mathfrak{u}_j=\mathfrak{g}_j+\mathfrak{g}_{j-s}, \tag{6.7.2}$$

where it is understood that $\mathfrak{g}_{-s}$ denotes the zero subspace.

It is an immediate consequence of (6.7.2) that z_0 is an eigenvector of P_0. In fact,

$$P_0z_0=\omega z_0. \tag{6.7.3}$$

But this clearly means that the Cartan subalgebra $\mathfrak{h}'=\mathfrak{g}^{z_0}$ is stable under P_0.

On the other hand, the elements $y_i = u_i + v_i$, where $u_i \in \mathfrak{g}_{k_i}$, form a basis of $\mathfrak{h}'$. Let us apply P_0 to these basal elements. Then by § 6. 5

$$P_0 y_i = \omega^{k_i} u_i + P_0 v_i.$$

But the elements $P_0 y_i$ belong to $\mathfrak{h}'$ and furthermore since, obviously, $P_0 v_i \in \mathfrak{n}^*$, it follows that

$$\rho_0(P_0 y_i) = \omega^{k_i} u_i.$$

But now if we apply Lemma 6. 4A we must have

$$P_0 y_i = \omega^{k_i} y_i.$$

Thus y_i, u_i and hence also v_i are contained in $\mathfrak{u}_{k_i}$. But since $v_i \in \mathfrak{n}^*$, it follows from (6. 7. 2) that $v_i \in \mathfrak{g}_{k_i - s}$. Thus not only did we prove that the v_i are eigenvectors of $\operatorname{ad} x_0$ but more we obtain a duality relation among the integers k_i.

LEMMA 6. 7. *Let v_i, $i = 1, 2, \cdots, l$, be defined by (6. 5. 2). Then $v_i \in \mathfrak{g}_{k_i - s}$, $i = 1, 2, \cdots, l$. Also the integers k_i satisfy the following duality law,*

$$s = k_1 + k_l = k_2 + k_{l-1} = \cdots = k_l + k_1.$$

Proof. Only the second part of Lemma 6. 7 is not yet proved. By Lemma 6. 6 the elements v_i are a basis of $\mathfrak{g}^{v_l}$ and the first part of Lemma 6. 7 asserts that v_i is an eigenvector of $\operatorname{ad} x_0$ with eigenvalue $k_i - s$. On the other hand, as we have seen, the eigenvalues of $\operatorname{ad} x_0$ on $\mathfrak{g}^{v_l}$ are, in non-decreasing order,

$$-k_l \leqq -k_{l-1} \leqq \cdots \leqq -k_1.$$

But these must be identical, and in the same order, as

$$k_1 - s \leqq k_2 - s \leqq \cdots \leqq k_l - s.$$

Subtracting termwise we obtain for all defined p, $k_p + k_{l+1-p} = s$. Q. E. D.

Observe that the duality together with the inequality $k_{l-1} < k_l$ implies the inequality $k_1 < k_2$.

In [3] Chevalley observed empirically a similar duality in the exponents (see [3], p. 24) of $\mathfrak{g}$. Later it will be proved that the integers k_i are in fact these exponents and that the duality observed in the latter is the same as the duality just proved in the former. More than just a numerical coincidence the duality in the k_i takes the following form. (Theorem 6. 7 summarizes results which have already been proved.)

THEOREM 6. 7. *Let c_i, $i = 1, 2, \cdots, l$, be l arbitrary non-zero complex*

numbers. Let q_i, $i = 1, 2, \cdots, l$, be the coefficients of the highest root ψ relative to the simple positive roots α_i.

Let

$$e_0 = \sum_{i=1}^{l} c_i e_{\alpha_i}$$

and

$$\tilde{e}_0 = \sum_{i=1}^{l} (q_i/c_i) e_{-\alpha_i}.$$

Then e_0 and $\tilde{e}_0$ are principal nilpotent elements in $\mathfrak{g}$ so that $\mathfrak{g}^{e_0}$ and $\mathfrak{g}^{\tilde{e}_0}$ are l-dimensional and commutative.

Let $x_0 = \sum_{i=1}^{l} \epsilon_i$, where ϵ_i, $i = 1, 2, \cdots, l$, is the basis of the Cartan subalgebra $\mathfrak{h}$ dual to the simple positive roots α_i, $i = 1, 2, \cdots, l$, so that $(x_0, \phi) = o(\phi)$ is the order of a root ϕ. For any non-zero integer j let

$$\mathfrak{g}_j = \sum_{o(\phi)=j} (e_\phi)$$

be the eigenspace of $\operatorname{ad} x_0$ *for the eigenvalue j.*

Then $\mathfrak{g}^{e_0}$ and $\mathfrak{g}^{\tilde{e}_0}$ are each stable under $\operatorname{ad} x_0$ *and the eigenvalues of the restriction of* $\operatorname{ad} x_0$ *to $\mathfrak{g}^{e_0}$ and $\mathfrak{g}^{\tilde{e}_0}$, respectively, are positive integers k_i and the negative integers $-k_i$, $i = 1, 2, \cdots, l$, where*

$$1 = k_1 < k_2 \leqq \cdots \leqq k_{l-1} < k_l = q,$$

and $q = \sum_{i=1}^{l} q_i = o(\psi)$ and $2k_1 + 1, 2k_2 + 1, \cdots, 2k_l + 1$ are the dimensions of the irreducible components occuring in the complete reduction of the representation of a principal TDS *on* $\mathfrak{g}$.

Let

$$z_0 = e_0 + e_{-\psi}$$

and

$$\tilde{z}_0 = \tilde{e}_0 + e_\psi$$

(cycle elements). Then z_0 and $\tilde{z}_0$ are regular, so that $\mathfrak{g}^{z_0}$ and $\mathfrak{g}^{\tilde{z}_0}$ are Cartan subalgebras; and $[z_0, \tilde{z}_0] = 0$ so that $\mathfrak{g}^{z_0} = \mathfrak{g}^{\tilde{z}_0}$.

Let P_0, a principal element of G, be given by $P_0 = \operatorname{Exp}(2\pi i/s) x_0$, where $s = q + 1$. Write $\mathfrak{h}'$ for $\mathfrak{g}^{z_0} = \mathfrak{g}^{\tilde{z}_0}$ Then $\mathfrak{h}'$ is orthogonal to $\mathfrak{h}$. But much more than this, $\mathfrak{h}'$ is stable under P_0 and the eigenvalues of $P_0 \mid \mathfrak{h}'$ are ω^{k_i}, $i = 1, 2, \cdots, l$, where $\omega = e^{2\pi i/s}$. Furthermore, we can find corresponding eigenvectors, y_i, which form a basis of $\mathfrak{h}'$ and are such that

$$y_i = u_i + v_i,$$

where the u_i form a basis of $\mathfrak{g}^{e_0}$ and the v_i form a basis of $\mathfrak{g}^{\tilde{e}_0}$, $i=1,2,\cdots,l$. Moreover, $u_i \in \mathfrak{g}_{k_i}$ and $v_i \in \mathfrak{g}_{k_i-s}$ so that the integers k_i satisfy the duality relation

$$s=k_1+k_l=k_2+k_{l-1}=\cdots=k_l+k_1.$$

Finally we can choose $y_1=z_0$ and $y_l=\tilde{z}_0$.

6.8. Among other things, Theorem 6.7 asserts that the integers k_i may be found by considering the eigenvalues, ω^{k_i}, of the restriction of the principal element P_0 to $\mathfrak{h}'$. Theorem 6.8 below asserts that without knowledge of $\mathfrak{h}'$ or the restriction $P_0 \mid \mathfrak{h}'$ we can determine the integers k_i directly by considering multiplicities of eigenvalues of a principal element with respect to its action on $\mathfrak{g}$. In the notation of § 6.4 and Theorem 6.8 this means we can express n_k in terms of s_k.

THEOREM 6.8. *Let P be a principal element of G. Let s_k, $k=0,1,\cdots,q$, be the multiplicity of the eigenvalue ω^k of P (In the notation of § 6.7, $s_k=\dim \mathfrak{g}_k+\mathfrak{g}_{k-s}$) and as in § 6.4 let n_k be the multiplicity of π_{2k+1} in the adjoint representation a principal* TDS *on $\mathfrak{g}$. Then*

$$n_k=s_k-l \tag{6.8.1}$$

In other words, let $\mathfrak{h}_1$ be a Cartan subalgebra which is stable under P and is such that the eigenvalues of $P \mid \mathfrak{h}_1$ are ω^{k_i}, $i=1,2,\cdots,l$ (such a Cartan subalgebra exists by Theorem 6.7). Then if $\mathfrak{m}_1$ is the B-orthocomplement to $\mathfrak{h}_1$, $\mathfrak{m}_1$ is stable under P and the eigenvalues of $P \mid \mathfrak{m}_1$ are ω^k, $k=0,1,\cdots,q$. Furthermore each eigenvalue of $P \mid \mathfrak{m}_1$ occurs with multiplicity l.

Proof. Since any element in G is orthogonal with respect to B, it follows that $\mathfrak{m}_1$ is stable under P. It suffices then to assume $P=P_0$ and $\mathfrak{h}_1=\mathfrak{h}$ to prove Theorem 6.8 for this case. Now by § 2.5(h)

$$\dim \mathfrak{g}_j-\dim \mathfrak{g}_{j+1}=n_j. \tag{6.8.2}$$

Since $n_0=0$ upon summing (6.8.2) we obtain for $0 \leq k \leq q$

$$\dim \mathfrak{g}_0-\dim \mathfrak{g}_k=\sum_{j=1}^{k-1} n_j. \tag{6.8.3}$$

But by § 2.5(f)

$$\dim \mathfrak{g}_{s-k}=\sum_{j=s-k}^{q} n_j. \tag{6.8.4}$$

But by the duality in Theorem 6.7 $n_{s-j}=n_j$. But then subtracting (6.8.3) from (6.8.4) and recalling that $\dim \mathfrak{g}_{s-k}=\dim \mathfrak{g}_{k-s}$ and $\dim \mathfrak{g}_0=l$ it follows that

$$s_k-l=\dim(\mathfrak{g}_k+\mathfrak{g}_{k-s})-l=n_k. \qquad \text{Q.E.D.}$$

COROLLARY 6.8. *Let r be the number of positive roots of $\mathfrak{g}$. Let $s = q+1$, where q is the order of the highest root ψ. Then*

$$ls = 2r.$$

Proof. This immediately follows from the second part of Theorem 6.8 since $\dim m_1 = 2r$. Q.E.D.

Since $n = l + 2r$ note that it also proved that l divides n. In fact $n = l(s+1)$.

7. The notion of the apposition of two Cartan subalgebras.

1. Let $\mathfrak{h}_1$ be any Cartan subalgebra of $\mathfrak{g}$. Let H_1 be the corresponding subgroup of G. Let $N(H_1)$ be the normalizer of H_1 in G. It is obvious that $A \in N(H_1)$ if and only if $\mathfrak{h}_1$ is stable under A. Let W_1 be the subgroup of endomorphisms of $\mathfrak{h}_1$ induced by restricting the elements of $N(H_1)$ to $\mathfrak{h}_1$. Then the restriction defines a homomorphism

$$\zeta : N(H_1) \to W_1$$

of $N(H_1)$ onto W_1. The group W_1 is finite and is called the Weyl group with respect to $\mathfrak{h}_1$. It is well known that the kernel of ζ is H_1 so that $N(H_1)/H_1 \cong W_1$. If $\sigma \in W_1$ and $A \in N(H_1)$ and $A \in N(H_1)$ is such that $\zeta(A) = \sigma$, then A will be called an extension of σ. It is clear then that the most general extension of σ is of the form A_1A, where $A_1 \in H_1$.

Let Δ_1 be the set of roots with respect to $\mathfrak{h}_1$. It is well known that Δ_1 is stable under W_1. For each root $\phi \in \Delta_1$ let R_ϕ be the "reflection" of $\mathfrak{h}_1$ defined by

$$R_\phi y = y - (2(\phi, y)/(\phi, \phi))\phi \tag{7.1.1}$$

One knows that $R_\phi \in W_1$ for all $\phi \in \Delta_1$ and that W_1 is generated by these reflections (See [12], Theorème 1, p. 16-05).

LEMMA 7.1. *Let $\sigma \in W_1$. Let μ be an eigenvalue of σ. Then μ is a primitive j-th root of unity for some j and every other primitive j-th root of unity occurs as an eigenvalue of σ.*

Proof. Since Δ_1 is stable under σ, there exists a basis of $\mathfrak{h}_1$ (e.g. a set of simple positive roots) with respect to which σ is represented by a matrix with rational coefficients. It follows then that the characteristic polynomial of σ also has rational coefficients. Now since σ has finite order, μ must be a primitive j-th root of unity for some integer j. It folows then that the characteristic polynomial of σ is a product of cyclotomic polynomials and

hence every primitive j-th root of unity is a root of the characteristic polynomial. Q. E. D.

7.2. Let $\mathfrak{u}_1$ and Π^Q, the set of Q-simple roots with respect to D, be defined, respectively, as in § 6.7 and § 6.2. It is clear that $\mathfrak{u}_1$ is the set of all elements $y \in \mathfrak{g}$ of the form

$$y = \sum_{\beta \in \Pi^Q} a_\beta e_\beta$$

We know that when all the coefficients a_β are different from zero, y is cyclic, and hence also regular. It is interesting that in case one of the coefficients is zero, not only does y cease to be regular, it is in fact nilpotent.

LEMMA 7.2. *Let Π^Q be as in § 6.2. Let $y \in \mathfrak{g}$ be of the form*

$$y = \sum_{\beta \in \Pi^Q} a_\beta e_\beta.$$

That is, in the notation of § 6.7, assume y satisfies $P_0 y = \omega y$. Then if one of the coefficients a_β is zero, y is nilpotent.

Proof. Assume one of the coefficients is zero. In fact, let β_i, $i = 1, 2, \cdots, l+1$, be the elements of Π^Q. Without loss assume $a_{\beta_{l+1}} = 0$.

Now upon writing $\psi = \sum_{i=1}^{l} q_i \alpha_i$ we know that the coefficients q_i are all non-zero (See (5.3.3)). It follows immediately then that the roots $\beta_1, \beta_2, \cdots, \beta_l$ form a basis of $\mathfrak{h}$. But if we use this basis to define a lexicographical ordering in $\mathfrak{h}^\#$ and set $\bar{\Delta}^+$ equal to the set of positive roots relative to this ordering, it follows that $\beta_i \in \bar{\Delta}^+$ for $i = 1, 2, \cdots, l$. But then $\bar{\mathfrak{n}} = \sum_{\phi \in \bar{\Delta}^+} (e_\phi)$ is a Lie algebra of nilpotent elements and $y \in \bar{\mathfrak{n}}$. Hence y is nilpotent. Q. E. D.

7.3. Applying Lemma 6.2 we obtain the corollary

LEMMA 7.3. *Let $y \in \mathfrak{u}_1$. Let H be the subgroup of G corresponding to $\mathfrak{h}$. Then y is either nilpotent or else there exists $A \in H$ and a non-zero scalar λ such that*

$$y = \lambda A z_0.$$

For any element $A \in G$ let $\mathfrak{g}^A$ be the set of fixed vectors of A. An element $A \in G$ is then said to be regular if (1) A is semi-simple (that is, A is diagonalizable) and (2) $\mathfrak{g}^A$ is a Cartan subalgebra. It follows from Theorem 6.8 that a principal element $P \in G$ is regular.

Now a special relation, to be defined below, exists between the pair of

orthogonal Cartan subalgebras $\mathfrak{h}$ and $\mathfrak{h}'$ (See Theorem 6.7). We will show that this relation defines $\mathfrak{h}$ and $\mathfrak{h}'$ uniquely up to conjugacy.

Let $\mathfrak{h}_1$ and $\mathfrak{h}'_1$ be two Cartan subalgebras of $\mathfrak{g}$. We will then say that $\mathfrak{h}'_1$ is in appostition to $\mathfrak{h}_1$ with respect to a principal element $P \in G$ if (1) $g^P = \mathfrak{h}_1$ and, (2) $\mathfrak{h}'_1$ is stable under P and the set of eigenvalues of $P \mid \mathfrak{h}'_1$ includes a primitive s root of unity. (Observe that the number s has special significance for a principal element; the order of a principal element in G equals s.)

By Theorem 6.7 it is clear that $\mathfrak{h}'$ is in apposition to $\mathfrak{h}$ with respect to P_0.

THEOREM 7.3. *Assume that the Cartan subalgebra $\mathfrak{h}'_1$ is in apposition to $\mathfrak{h}_1$ with respect to the principal element P_1 and that $\mathfrak{h}'_2$ is in apposition to $\mathfrak{h}_2$ with respect to P_2. Then there exists $A \in G$ such that $AP_1A^{-1} = P_2$, $A\mathfrak{h}_1 = \mathfrak{h}_2$, and $A\mathfrak{h}'_1 = \mathfrak{h}'_2$.*

Proof. It suffices to assume $P_1 = P_0$, $\mathfrak{h}_1 = \mathfrak{h}$ and $\mathfrak{h}'_1 = \mathfrak{h}'$. Now all principal elements in G are conjugate to each other. Hence there exists $A_1 \in G$ such that $A_1P_0A_1^{-1} = P_2$. Since $\mathfrak{g}^{P_2} = \mathfrak{h}_2$, it is obvious that $A_1\mathfrak{h} = \mathfrak{h}_2$. Thus it also suffices to assume $\mathfrak{h}_2 = \mathfrak{h}$ and $P_2 = P_0$. But now $\mathfrak{h}'_2$ is stable under P_0 and $P_0 \mid \mathfrak{h}'_2$ has a primitive s root of unity as an eigenvalue. By Lemma 7.1 ω is also an eigenvalue of $P_0 \mid \mathfrak{h}'_2$. Let $y \in \mathfrak{h}'_2$, $y \neq 0$, be a corresponding eigenvector. Then in the notation of § 6.7, $y \in \mathfrak{u}_1$. But since y is contained in a Cartan subalgebra, y is not nilpotent. Hence by Lemma 7.3 there exists $A \in G$ and a non-zero scalar λ such that $y = \lambda A z_0$. But then by Corollary 6.4 y is regular and hence $A\mathfrak{h}' = \mathfrak{h}'_2$. Q.E.D.

8. The Coxeter-Killing transformation.

1. An element $\gamma' \in W$ will be called a transformation of Coxeter-Killing if it can be put in the form

$$\gamma' = R_{\alpha'_1} R_{\alpha'_2} \cdots R_{\alpha'_l},$$

where α'_i, $i = 1, 2, \cdots, l$, are the simple positive roots, in some order, relative to some Weyl chamber in $\mathfrak{h}^\#$. In recent years this transformation has been studied by Coxeter. Relationships between the eigenvalues of this transformation and the eigenvalues of the matrix of Cartan integers have been established. (See [5]). Also one knows that all the transformations of Coxeter-Killing in W form a conjugate class in W.

Let $\gamma = R_{\alpha_1} R_{\alpha_2} \cdots R_{\alpha_l}$. An integral valued function on the Weyl group,

which plays an important role in the cohomolgy theory of complex homogeneous spaces and also of $\mathfrak{n}$ is the function $N(\sigma)$ which assigns to each $\sigma \in W$ the number of positive roots which go over into negative roots under the action of σ. The knowledge of $N(\gamma)$ will play an essential role in proving that the order of γ is s.

THEOREM 8.1. *Let γ be the transformation of Coxeter-Killing defined by letting $\gamma = R_{\alpha_1} R_{\alpha_2} \cdots R_{\alpha_l}$. Then $N(\gamma) = l$. Furthermore if ϕ_i, $i = 1, 2, \cdots, l$, are the positive roots which change sign under γ then the roots ϕ_i form a basis of $\mathfrak{h}$.*

Proof. Let ϕ_i, $i = 1, 2, \cdots, l$, be defined by

$$\phi_i = R_{\alpha_l} R_{\alpha_{l-1}} \cdots R_{\alpha_{i+1}} \alpha_i.$$

It follows easily from (7.1.1) that

$$\phi_i = \alpha_i + \sum_{j>i} c_{ij} \alpha_j.$$

Since the coefficient of α_i in ϕ_i is one, it follows that ϕ_i is positive. Furthermore, since the coefficient of α_j in ϕ_i for $j < i$ is zero, it is clear that ϕ_i are linearly independent and hence form a basis of $\mathfrak{h}$.

But clearly

$$\gamma(\phi_i) = R_{\alpha_1} R_{\alpha_2} \cdots R_{\alpha_{i-1}} (-\alpha_i)$$

and hence

$$\gamma(\phi_i) = -\alpha_i + \sum_{j<i} c'_{ij} \alpha_j.$$

Since the coefficient of α_i in $\gamma(\phi_i)$ is minus one, ϕ_i is a positive root which changes sign under γ. Thus $N(\gamma) \geqq l$.

Now it is well known that $N(R_{\alpha_i}) = 1$. In fact, α_i is the only positive root which changes sign under R_{α_i}. This is clear since only the coefficient of α_i in ϕ, for any $\phi \in \Delta$, is affected by R_{α_i}.

Now assume ϕ is a positive root which changes sign under γ. Since $\gamma(\phi) \in \Delta^-$, there clearly exists a maximal value i such that

$$R_{\alpha_i} R_{\alpha_{i+1}} \cdots R_{\alpha_l} \phi \in \Delta^-.$$

That is, $R_{\alpha_{i+1}} \cdots R_{\alpha_l} \phi \in \Delta^+$. It follows then that

$$\alpha_i = R_{\alpha_{i+1}} \cdots R_{\alpha_l} \phi.$$

This, however, means that $\phi = \phi_i$. Thus $N(\gamma) = l$. Q.E.D.

Now it is well known that one is not an eigenvalue of a Coxeter-Killing transformation. A proof of this resting on the work of Coxeter is given, for

example, in [4]. (See [4], p. 352). However, since a direct proof of this fact, making use of Theorem 8.1, can be given we shall include it.

LEMMA 8.1. *Let γ be the Coxeter-Killing transformation given as in* § 8.1. *Then one is not an eigenvalue of* γ.

Proof. Let ϵ_i, $i=1,2,\cdots,l$, be the basis of $\mathfrak{h}$ given as in § 5.1. Let $\epsilon'_i = 2\epsilon_i/(\alpha_i,\alpha_i)$. Clearly

$$\begin{aligned}\gamma\epsilon'_i &= R_{\alpha_1}\cdots R_{\alpha_i}\epsilon'_i\\ &= \epsilon'_i + R_{\alpha_1}\cdots R_{\alpha_{i+1}}(-\alpha_i)\end{aligned}$$

by (7.1.1). On the other hand, it is clear from the definition of ϕ_i in the proof of Theorem 8.1 that $R_{\alpha_1}\cdots R_{\alpha_{i+1}}(-\alpha_i) = \gamma(\phi_i)$. Thus we have

$$\gamma\epsilon'_i = \epsilon'_i + \gamma(\phi_i).$$

Assume now that $x \in \mathfrak{h}$ is fixed under γ. Write $x = \sum_{i=1}^{l} a_i\epsilon'_i$. Then

$$\begin{aligned}x &= \gamma x\\ &= \sum_{i=1}^{l} a_i(\epsilon'_i + \gamma(\phi_i))\\ &= x + \sum_{i=1}^{l} a_i\gamma(\phi_i).\end{aligned}$$

Thus $\sum_{i=1}^{l} a_i\gamma(\phi_i) = 0$. However, by Theorem 8.1 the vectors ϕ_i and hence $\gamma(\phi_i)$ are linearly independent. Thus $a_i = 0$, $i=1,2,\cdots,l$, and hence $x=0$. Q.E.D.

8.2. Lemma 8.1 is needed solely to prove

LEMMA 8.2. *Let $\Gamma_i \subseteq \Delta$, $i=1,2,\cdots,L$, be the orbits in Δ under the action of γ. Then for $i=1,2,\cdots,L$*

$$\sum_{\phi\in\Gamma_i}\phi = 0.$$

Proof. This follows immediately from Lemma 8.1 since the sum of the roots in any orbit of γ is obviously left fixed by γ. Q.E.D.

The following theorem is proved in [4]

THEOREM 8.2 (Coleman). *Let h be the order of the Coxeter-Killing transformation γ defined as in* § 8.1. *Let $\nu = e^{2\pi i/h}$. Then there exists a regular eigenvector z_1 of γ whose corresponding eigenvalue is ν.*

Coleman also observed and used in [4] the following consequence of Theorem 8.2. We repeat his proof.

COROLLARY 8.2. *As in Lemma* 8.2 *let* $\Gamma_i \subseteq \Delta$, $i=1,2,\cdots,L$, *denote the distinct orbits of* γ *with respect to its action on the set of roots* Δ. *Then each orbit* Γ_i *contains exactly* h *roots so that in particular* $hL=2r$, *where* $2r$ *is the total number of roots.*

Proof. Let $\phi \in \Delta$. Assume $\gamma^m\phi=\phi$. It suffices to prove that h divides m. Now, where z_1 is given as in Theorem 8.2,

$$\begin{aligned}(z_1,\phi) &= (z_1,\gamma^m\phi)\\ &= (\gamma^{-m}z_1,\phi)\\ &= \nu^{-m}(z_1,\phi).\end{aligned}$$

But since z_1 is regular, $(z_1,\phi)\neq 0$ and hence $\nu^{-m}=1$. This implies h divides m. Q.E.D.

8.3. Now one knows that the Poincaré polynomial $P_G(t)$ can be put in the form

$$P_G(t)=(1+t^{2m_1+1})(1+t^{2m_2+1})\cdots(1+t^{2m_l+1}),$$

where the m_i, $i=1,2,\cdots,l$, are positive integers in non-decreasing order. The integers m_i (sometimes m_i+1) are called the exponents of $\mathfrak{g}$ (or W as in [4]). When the values of the exponents for the simple exceptional Lie algebras were announced by Chevalley at the International Congress at Cambridge in 1950, Coxeter recognized a rather remarkable coincidence. He observed (1) that in all cases $hl=2r$, so that in our notation $h=s$, and hence $\nu=\omega$ (See Corollary 6.8), (2) $m_i\leqq h$ and (3) the eigenvalues of γ are ω^{m_i}, $i=1,2,\cdots,l$. No proofs were given and the question of obtaining a proof remained open until recently. In [4], using $hl=2r$ as the only empirically observed fact, Coleman proved that $m_i\leqq h$ and that the eigenvalues of a Coxeter-Killing transformation are indeed ω^{m_i}, $i=1,2,\cdots,l$. To make the proof independent of any empirical information Coleman states that it would be desirable to prove that $hl=2r$, that is, to prove that the number L of orbits in Δ under the action of γ equals l. (See Corollary 8.2.) Another open question, stated in [4], is proving that $h=q+1$, where q is the order of the highest root. (See [4], p. 356.) But since by definition $s=1+q$, it is clear from Corollary 6.8 that both of these questions are settled when it is shown that $h=s$. The statement that $h=s$ is a part of Theorem 8.4 below.

8.4. Now let γ be defined as in § 8.1. Let $A_\gamma \in G$ be any extension of γ. Let $\Gamma_i\subseteq\Delta$, $i=1,2,\cdots,L$, be defined as in § 8.2 and let

$$\mathfrak{b}_i=\sum_{\phi\in\Gamma_i}(e_\phi). \qquad (8.4.1)$$

By Corollary 8.2 it is clear that each subspace $\mathfrak{b}_i$ is of dimension h. Furthermore, since

$$A_\gamma((e_\phi)) = (e_{\gamma\phi})$$

for any $\phi \in \Delta$, it is clear that

$$\mathfrak{g} = \mathfrak{h} + \sum_{i=1}^{L} \mathfrak{b}_i$$

is a direct sum decomposition of $\mathfrak{g}$ into subspaces which are stable under A_γ.

Now since γ^h is the identity element of W, we can define the scalar λ_ϕ, for any root ϕ, by the relation

$$(A_\gamma)^h e_\phi = \lambda_\phi e_\phi. \tag{8.4.2}$$

By applying A_γ to both sides of (8.4.2) it is clear that $\lambda_\phi = \lambda_{\gamma\phi}$ for all ϕ. Now since $A_\gamma{}^h$ reduces to the identity on $\mathfrak{h}$, we can write $A_\gamma{}^h = \operatorname{Exp} x$ for some $x \in \mathfrak{h}$. It follows that $\lambda_\phi = e^{(x,\phi)}$ for any $\phi \in \Delta$. But then

$$\begin{aligned}(\lambda_\phi)^h &= \prod_{i=0}^{h-1} \lambda_{\gamma^i\phi} \\ &= e^{(x,\phi+\gamma\phi+\cdots+\gamma^{h-1}\phi)} \\ &= 1\end{aligned}$$

by Lemma 8.2. Thus λ_ϕ is an h root of unity. This shows that $A_\gamma{}^{2h} = 1$. We can now prove that $h = s$ and hence that $L = l$. More than this we have

THEOREM 8.4. *Let γ be a Coxeter-Killing transformation on the Cartan subalgebra $\mathfrak{h}$. Let h be the order of γ. Then $h = 1 + \sum_{i=1}^{l} q_i$, where the integers q_i are the coefficients of the highest root relative to a basis of simple positive roots. That is, $h = s$. Moreover, $hl = 2r$, where r is the number of positive roots so that there are l distinct orbits $\Gamma_i \subseteq \Delta$, $i = 1, 2, \cdots, l$, in Δ under the action of γ and each orbit contains h roots. Furthermore, if we take $\gamma = R_{\alpha_1} R_{\alpha_2} \cdots R_{\alpha_l}$ and let ϕ_i, $i = 1, 2, \cdots, l$, be the positive roots which change sign under γ (see Theorem 8.1), then we can choose an ordering of the orbits so that $\phi_i \in \Gamma_i$, $i = 1, 2, \cdots, l$.*

Now let $A_\gamma \in G$ be any extension of γ. Then $A_\gamma{}^h = 1$. That is, $A_\gamma{}^h e_\phi = e_\phi$ for any $\phi \in \Delta$ so that we can renormalize the root vectors e_ϕ in such a way that

$$A_\gamma{}^i e_\phi = e_{\gamma^i\phi}$$

for any $\phi \in \Delta$ and any integer i.

Now let $w_i \in \mathfrak{g}$, $i = 1, 2, \cdots, l$, be defined by

$$w_i = \sum_{\phi \in \Gamma_i} e_\phi$$

and let $\mathfrak{h}$ be the subspace spanned by the elements w_i. Then $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$ (so that the elements w_i are semisimple and commute with each other). Furthermore, $\bar{\mathfrak{h}} = \mathfrak{g}^{A_\gamma}$.

Proof. Let γ, A_γ and λ_ϕ for $\phi \in \Delta$ be as previously defined. It has been shown that $A_\gamma^{2h} = 1$. In particular A_γ is semisimple. But if $A \in G$ is semisimple it is well known that $\mathfrak{g}^A$ contains a Cartan subalgebra of $\mathfrak{g}$ (See e.g. [8]). For $A = A_\gamma$ the proof is somewhat more direct since A_γ, having finite order, lies in a maximal compact subgroup of G. But then $A_\gamma = \operatorname{Exp} x$ for some x in a compact form of $\mathfrak{g}$. We could then apply § 6.1(d)). Let $\bar{\mathfrak{h}}$ be a Cartan subalgebra of $\mathfrak{g}$ contained in $\mathfrak{g}^{A_\gamma}$.

Now let $\mathfrak{b}_i$, $i = 1, 2, \cdots, L$, be defined by (8.4.1). Consider the decomposition

$$\mathfrak{g} = \mathfrak{h} + \sum_{i=1}^{L} \mathfrak{b}_i.$$

Obviously

$$\begin{aligned} \mathfrak{g}^{A_\gamma} &= \mathfrak{h} \cap \mathfrak{g}^{A_\gamma} + \sum_{i=1}^{L} \mathfrak{b}_i \cap \mathfrak{g}^{A_\gamma} \\ &= \sum_{i=1}^{L} \mathfrak{b}_i \cap \mathfrak{g}^{A_\gamma} \end{aligned} \tag{8.4.3}$$

by Lemma 8.1.

Now let $\phi \in \Gamma_i$. As we have already noted $\lambda_\phi = \lambda_{\gamma^i \phi}$ for any integer i. Thus A_γ^h reduces to the scalar λ_ϕ on the space $\mathfrak{b}_i$. But then if $\lambda_\phi \neq 1$, A_γ^h has no non-zero fixed vectors in $\mathfrak{b}_i$ and hence certainly $\mathfrak{b}_i \cap \mathfrak{g}^{A_\gamma} = 0$. On the other hand, if $\lambda_\phi = 1$, then clearly $\mathfrak{b}_i \cap \mathfrak{g}^{A_\gamma}$ is the one dimensional subspace spanned by $\sum_{i=0}^{h-1} A_\gamma{}^i e_\phi$. Thus if L_1 is the number of integers i, $1 \leqq i \leqq L$, such that $\lambda_\phi = 1$ for all $\phi \in \Gamma_i$, it follows from (8.4.3) that $L_1 = \dim \mathfrak{g}^{A_\gamma}$. In fact, since $\mathfrak{h} \subseteq \mathfrak{g}^{A_\gamma}$, we then have

$$L \geqq L_1 = \dim \mathfrak{g}^{A_\gamma} \geqq l$$

and hence in particular $L \geqq l$.

Now we assert that for any i, $\Gamma_i \cap \Delta^+$ and $\Gamma_i \cap \Delta^-$ are both non-empty. Indeed assume, without loss, that $\Gamma_i \cap \Delta^-$ is empty. Then $\sum_{\phi \in \Gamma_i} \phi$, in the lexicographical order of $\mathfrak{h}^\#$, must be strictly positive and hence cannot vanish. This contradicts Lemma 8.1 and hence the assertion is proved. Now since $\Gamma_i \cap \Delta^+$ and $\Gamma_i \cap \Delta^-$ are non-empty, it is clear that there exists a root $\phi \in \Gamma_i \cap \Delta^+$ such that $\gamma\phi \in \Gamma_i \cap \Delta^-$. That is, each orbit Γ_i contains at least one positive root which changes sign under γ. But then if we apply Theorem 8.1 it follows obviously that $L \leqq l$. Thus $L = L_1 = \dim \mathfrak{g}^{A_\gamma} = l$. That is, $\lambda_\phi = 1$ for all $\phi \in \Delta$ and $\mathfrak{g}^{A_\gamma} = \bar{\mathfrak{h}}$. Furthermore, if the root vectors e_ϕ, $\phi \in \Delta$,

are normalized so that $A_\gamma e_\phi = e_{\gamma\phi}$, it follows that the vectors $w_i = \sum_{\phi \in \Gamma_i} e_\phi$ form a basis of $\mathfrak{g}^{A_\gamma}$. Finally, observe that since $L = l$, each orbit Γ_i contains exactly one positive root which changes sign under γ. Q. E. D.

8.5. Let A_γ be as in Theorem 8.4. As we have noted in § 8.3 the eigenvalues of the restriction γ of A_γ to $\mathfrak{h}$ are the numbers ω^{m_i}, $i = 1, 2, \cdots, l$, where the m_i are the exponents of $\mathfrak{g}$. Let $\mathfrak{m}$ be the B-orthogonal complement to $\mathfrak{h}$ in $\mathfrak{g}$. It is clear that $\mathfrak{m}$ is stable under A_γ. Theorem 8.4 enables us to determine the eigenvalues of A_γ on $\mathfrak{m}$.

COROLLARY 8.5. *Let A be any extension of the Coxeter-Killing transformation γ and let the root vectors be normalized so that $Ae_\phi = e_{\gamma\phi}$ for all $\phi \in \Delta$. Let $\omega = e^{2\pi i/s}$ and let the roots ϕ_i be defined as in Theorem 8.1. Define for $i = 1, 2, \cdots, l$, $j = 1, 2, \cdots, s$,*

$$y^j{}_i = \sum_{k=0}^{h-1} \bar{\omega}^{jk} e_{\gamma^k \phi_i}.$$

Then $y^j{}_i$ is a basis of the B-orthogonal complement $\mathfrak{m}$ to the Cartan subalgebra $\mathfrak{h}$ in $\mathfrak{g}$ and

$$A_\gamma y^j{}_i = \omega^j y^j{}_i$$

for all given values of i and j. In particular, the eigenvalues of A_γ on $\mathfrak{m}$ are ω^j, $j = 0, 1, \cdots, s-1$, and each eigenvalue occurs with multiplicity l.

Proof. This is an immediate consequence of Theorem 8.4 which asserts that A_γ on any of the subspaces $\mathfrak{b}_i$ permutes the basal elements $e_{\gamma^k\phi_i}$, $k = 1, 2, \cdots, s-1$, according to the cyclic permutation $(1, 2, \cdots, s)$. Q. E. D.

8.6. Upon comparing Corollary 8.5 with Theorem 6.8 the suggestion arises that perhaps A_γ is a principal element of $\mathfrak{g}$ and that $\mathfrak{h}$ is in apposition to $\mathfrak{g}^{A_\gamma}$ with respect to A_γ. This is in fact the case as Theorem 8.6 states.

As in Theorem 8.4 write $\tilde{\mathfrak{h}}$ for the Cartan subalgeba $\mathfrak{g}^{A_\gamma}$. Then since all the elements of $\tilde{\mathfrak{h}}$ are fixed by A_γ, there exists an element $w \in \tilde{\mathfrak{h}}$ such that

$$A_\gamma = \operatorname{Exp} w.$$

However, such an element w is not unique. We will have to choose w correctly in order to prove Theorem 8.6.

Let $A \in G$ be such that $A\mathfrak{h} = \mathfrak{h}$. Hereafter, the addition of the symbol $(\sim)$ to previous notation designates the effect of applying the automorphism A. Now let Y designate the infinite discrete group of translations in $\tilde{\mathfrak{h}}$ by all vectors of the form $\sum_{i=1}^{l} t_i \tilde{\epsilon}_i$, where the coefficients t_i are integers and ϵ_i,

$i=1,2,\cdots,l$, are defined as in § 5.1. It is then easy to prove and well known fact that for x and $y \in \tilde{\mathfrak{h}}$, $\operatorname{Exp} 2\pi ix = \operatorname{Exp} 2\pi iy$ if and only if there exists $\delta \in Y$ such that $\delta x = y$.

For any $\sigma \in W$ and $\delta \in Y$ it is obvious that $\sigma\delta\sigma^{-1} \in Y$. It follows that if Z is the set of all linear transformations of $\tilde{\mathfrak{h}}$ of the form $\delta\sigma$, $\delta \in Y$, $\sigma \in \tilde{W}$, then Z is a group (a semi-direct product of Y and W). It is well known and not difficult to show that for any $x, y \in \tilde{\mathfrak{h}}$, $\operatorname{Exp} 2\pi ix$ is conjugate by an element in $N(\tilde{H})$, the normalizer of $\tilde{H}$, to $\operatorname{Exp} 2\pi iy$ if and only if there exists $\eta \in Z$ such that $\eta x = y$. (See [14], Theorem 6, p. 177).

Consider the action of Z on $\tilde{\mathfrak{h}}^{\#}$. Let

$$T = \{y \in \tilde{\mathfrak{h}} \mid (\tilde{\alpha}_i, y) \geqq 0, (\tilde{\psi}, y) \leqq 1 \text{ for } i=1,2,\cdots,l\}. \tag{8.6.1}$$

The set T is called the funadmental simplex of the chamber $\tilde{D}$. As one knows T has the property that given any $y \in \tilde{\mathfrak{h}}^{\#}$ there exists $x \in T$ and $n \in Z$ such that $\eta x = y$. (See [14], Theorem p. 177 and Theorem 8, p. 180). As a consequence, if we define

$$U = \bigcup_{\sigma \in W} \sigma T,$$

then since $Z = Y\tilde{W}$, given any $y \in \tilde{\mathfrak{h}}^{\#}$, there exists $x \in U$, $\delta \in Y$ such that $\delta x = y$. That is, there exists $x \in U$ such that $\operatorname{Exp} 2\pi ix = \operatorname{Exp} 2\pi iy$. Now we can write $A_\gamma = \operatorname{Exp} 2\pi iy$ for some $y \in \tilde{\mathfrak{h}}$. However, since the eigenvalues of A_γ have modulus one it follows that (y, ϕ) must be real for every $\phi \in \tilde{\Delta}$. Thus y must be contained in $\tilde{\mathfrak{h}}^{\#}$. But then by what we have just seen we can choose $x \in U$ so that $A_\gamma = \operatorname{Exp} 2\pi ix$. But then $x \in \sigma T$ for some $\sigma \in \tilde{W}$. Now our choice of A was arbitrary except only that $A\mathfrak{h} = \tilde{\mathfrak{h}}$. Without loss of generality then (modification of A) we can assume that $\sigma = 1$. That is, for a suitable choice of A we have

$$A_\gamma = \operatorname{Exp} 2\pi ix$$

for some $x \in T$.

Now by Theorem 8.4 all eigenvalues of A_γ are s roots unity. Thus if we write

$$x = \sum_{i=1}^{l} (b_i/s)\tilde{\epsilon}_i$$

then the scalars b_i are non-negative integers. But now since $(\tilde{\psi}, x) \leqq 1$, it follows from (6.3.1) that

$$\sum_{i=1}^{l} q_i b_i/s \leqq 1. \tag{8.6.2}$$

But we have more information than this. By Theorem 8.4 A_γ is regular. Thus (ϕ, x) cannot be an integer for any $\phi \in \tilde{\Delta}$. Thus the strict inequality holds in (8.6.2). Furthermore, $b_i > 0$. Hence we conclude

$$b_i \geqq 1$$

and

$$s > \sum_{i=1}^{l} q_i b_i.$$

But $s - 1 = q = \sum_{i=1}^{l} q_i$ (see (6.3.1)). Hence it follows that $b_i = 1$ for all i. That is,

$$x = \sum \tilde{\epsilon}_i / s$$

or

$$x = \tilde{x}_0 / s$$

But $\tilde{x}_0$ is a principal regular element of $\mathfrak{g}$ and

$$A_\gamma = \operatorname{Exp} (2\pi i/s) \tilde{x}_0.$$

Thus A_γ is a principal element of G. In fact $A_\gamma = APA^{-1}$. Furthermore, since the restriction γ of A_γ to $\mathfrak{h}$ has ω for an eigenvalue, it follows by definition (See § 7.3) that $\mathfrak{h}$ is in apposition to $\bar{\mathfrak{h}}$ with respect to A_γ. We have proved

THEOREM 8.6. *Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$. Let W be the Weyl group operating on $\mathfrak{h}$ and let $\gamma \in W$ be a Coxeter-Killing transformation. That is, $\gamma = R_{\alpha_1} R_{\alpha_2} \cdots, R_{\alpha_l}$, where α_i, $i = 1, 2, \cdots, l$, are simple positive roots relative to some lexicographical order in $\mathfrak{h}^{\#}$ and $R_{\alpha_i} \in W$ are the reflections they define.*

Let A_γ be any element of the adjoint group G of $\mathfrak{g}$ which extends γ. Then A_γ is a principal element of G (so that in particular its order is s and all such extensions are conjugate to each other). Let $\bar{\mathfrak{h}}$ be the set of fixed elements of A_γ. Then $\bar{\mathfrak{h}}$ is a Cartan subalgebra (since principal elements are regular) and $\mathfrak{h}$ is in apposition to $\bar{\mathfrak{h}}$ with respect to A_γ (see § 7.3).

We derive a number of corollaries. The first is an immediate consequence of Theorem 7.3 and Theorem 8.6.

COROLLARY 8.6. *Let $\mathfrak{h}_1$ and $\mathfrak{h}'_1$ be Cartan subalgebras. Assume that $\mathfrak{h}'_1$ is in apposition to $\mathfrak{h}_1$ with respect to the principal element $P \in G$. Then the restriction of P to $\mathfrak{h}'_1$ defines a Coxeter-Killing transformation of $\mathfrak{h}'_1$. In particular, the restriction of P_0 to $\mathfrak{h}'$ is a Coxeter-Killing transformation (See Theorem 6.7).*

8.7. In § 9.2 we obtain a more general result (Theorem 9.2) than Corollary 8.6.

Taking § 2.5(h) into account the next corollary asserts the validity of the empirical method found by A. Shapiro for the determination of the exponents m_i.

COROLLARY 8.7. *For $i = 1, 2, \cdots, l$ let k_i be as given as in § 6.5 and*

let m_i be the exponents of $\mathfrak{g}$ in non-decreasing order. Then $k_i = m_i$, $i = 1, 2, \cdots, l$.

In other words, if d_i, $i = 1, 2, \cdots, l$, are the dimensions of the irreducible components of the adjoint representation of a principal TDS *on $\mathfrak{g}$, then*

$$\prod_{i=1}^{l} (1 + t^{d_i})$$

is the Poincaré polynomial of G.

Proof. This is an immediate consequence of the theorem of Coleman (see § 8. 3), Theorem 8. 4, Theorem 6. 7 and Corollary 8. 6. Q. E. D.

The proof of Theorem 8. 6 yields a characterization of principal elements of G. We know that a principal element of G is regular and that its order is s. Among all regular elements in G we now show that its order is minimal.

COROLLARY 8. 6. *Let $A \in G$ be regular and let k be its order (possibly ∞). Then $k \geqq s$, where $s = 1 + q$ and q is the order of the highest root. Furthermore, $k = s$ if and only if A is a principal element of G.*

Proof. It suffices to assume the order k of A is finite. Now $\mathfrak{g}^A$ is a Cartan subalgebra. Without loss we may assume this to be $\mathfrak{h}$. Since A has finite order the eigenvalues of A have modulus 1. Thus we may write $A = \operatorname{Exp} 2\pi i x$, where $x \in \mathfrak{h}^{\#}$. More than this, as argued in the proof of Theorem 8. 6, by conjugating A, if necessary, we may asume x is contained in the fundamental simplex of the chamber D. That is, $(x, \alpha_i) \geqq 0$, $i = 1, 2, \cdots, l$, $(x, \psi) \leqq 1$. On the other hand, since A is regular, (x, ϕ) is not an integer for any $\phi \in \Delta$ so that strict inequalities hold in the inequalities just given. Thus we may write $x = \sum_{i=1}^{l} (t_i/k)\epsilon_i$, where the t_i are positive integers and $\sum_{i=1}^{l} t_i q_i < k$. But then

$$s - 1 = \sum_{i=1}^{l} q_i \leqq \sum_{i=1}^{l} t_i q_i < k$$

which proves $s \leqq k$. Also if $k = s$ then $t_i = 1$ for $i = 1, 2, \cdots, l$. But in such a case A is clearly principal. In fact $A = P_0$.

9. A theorem on automorphisms and a characterization of cyclic elements.

1. Let $S^*(\mathfrak{g})$ be the algebra of all polynomials on $\mathfrak{g}$ (the symmetric algebra over the dual space to $\mathfrak{g}$). We may write $S^*(\mathfrak{g}) = \sum_{k=0}^{\infty} S^k(\mathfrak{g})$, where

$S^k(\mathfrak{g})$ is a space of homogeneous polynomials of degree k. The group G operates on $S^*(\mathfrak{g})$ by the relation

$$A(F)(x) = F(A^{-1}x), \tag{9.1.1}$$

where $A \in G$, $F \in S^*(\mathfrak{g})$, $x \in \mathfrak{g}$. Let $J^*(\mathfrak{g}) \subseteq S^*(\mathfrak{g})$ be the algebra of polynomials which are left fixed by all $A \in G$ and let $J^k(\mathfrak{g}) = S^k(\mathfrak{g}) \cap J^*(\mathfrak{g})$. Then it is due to Chevalley that $J^*(\mathfrak{g})$ is generated by l algebraically independent homogeneous polynomials I_j, $j = 1, 2, \cdots, l$. Furthermore, if $I_j \in J^{p_j}(\mathfrak{g})$, where $p_1 \leqq p_2 \leqq \cdots \leqq p_l$, then $p_i = m_i + 1$. (See [3] and also [2].)

The following lemma is an immediate consequence of this result of Chevalley and Corollary 8.7.

LEMMA 9.1. *Let I_j, $j = 1, 2, \cdots, l$, be the invariant polynomials defined as above. Then* $\deg I_l = s$ *and* $\deg I_j < s$ *for all* $j < l$.

Now let $J^*_+(\mathfrak{g})$ be the hyperplane in $J^*(\mathfrak{g})$ consisting of all polynomials in $J^*(\mathfrak{g})$ with zero constant term. Consider the variety in $\mathfrak{g}$ formed by the zeros of all polynomials in $J^*_+(\mathfrak{g})$. As one might expect,

THEOREM 9.1. *Let $x \in \mathfrak{g}$. Then $F(x) = 0$ for all $F \in J^*_+(\mathfrak{g})$ if and only if x is nilpotent.*

Proof. Let $F_k \in S^k(\mathfrak{g})$ be defined by

$$F_k(y) = \operatorname{trace}(\operatorname{ad} y)^k.$$

It is clear that $F_k \in J^k(\mathfrak{g})$. It is also clear that if x is not nilpotent $F_k(x) \neq 0$ for some integer k. Hence to prove Theorem 9.1 it must be shown, conversely, that if x is nilpotent, $F(x) = 0$ for all $F \in J^*(\mathfrak{g})$. Assume then that x is nilpotent. By Lemma 3.3 there exists $y \in \mathfrak{g}$ such that $[y, x] = x$. Let λ be an arbitrary non-zero real scalar and let $A^\lambda = \operatorname{Exp} \lambda y$. Clearly $A^\lambda x = e^\lambda x$. Now let $F \in J^k(\mathfrak{g})$. Obviously by (9.1.1)

$$F(x) = F(A^\lambda x) = F(e^\lambda x) = e^{k\lambda} F(x).$$

But $e^{k\lambda} \neq 1$. Thus $F(x) = 0$. This proves Theorem 9.1 since $J^*(\mathfrak{g})$ is generated by homogeneous polynomials. Q. E. D.

9.2. In the proof of Theorem 9.1 we have seen that if x is nilpotent and c is any non-zero scalar, there exists an automorphism $A \in G$ such that $Ax = cx$. The situation as Theorem 9.2 indicates is entirely different when x is not nilpotent. If x is cyclic, it has been shown (see Theorem 6.7) that there exists a principle element $P \in G$ such that $Px = \mu x$, where μ is a primitive

s root of unity. Among all possible relations of the form $Ax = cx$, where $A \in G$, and x is not nilpotent it will be shown that this is, in a very definite way, the critical case.

THEOREM 9.2. *Assume $A \in G$, $x \in \mathfrak{g}$ and $Ax = cx$. Assume further that x is not nilpotent. Then c is a primitive m-th root of unity for some integer m. Furthermore, m divides $m_j + 1$ for some exponent m_j of $\mathfrak{g}$ so that in particular $m \leqq s$. Finally, if $m = s$, then (1) x is a cyclic element of $\mathfrak{g}$ and (2) A is a principal element of G. Moreover, if $\mathfrak{h}_1$ is the Cartan subalgebra which contains x (cyclic implies regular), then $\mathfrak{h}_1$ is stable under A and the restriction σ of A to $\mathfrak{h}_1$ is a Coxeter-Killing transformation.*

Proof. Since x is not nilpotent, it follows from Theorem 9.1 that there exists j, $1 \leqq j \leqq l$, such that $I_j(x) \neq 0$. But

$$I_j(x) = I_j(Ax) = I_j(cx) = c^{p_j} I_j(x).$$

Thus $c^{p_j} = 1$. This proves that c is a primitive m-th root of unity, where m is an integer which divides $p_j = m_j + 1$. By Lemma 9.1, $m < s$.

Now let $S^*(\mathfrak{h})$ be the algebra of polynomials on $\mathfrak{h}$ and let $J^*(\mathfrak{h})$ be the subalgebra of all polynomials which are fixed under the action of the Weyl group W. Let $\tilde{\chi}: S^*(\mathfrak{g}) \to S^*(\mathfrak{h})$ be the homomorphism defined by restricting a polynomial on $\mathfrak{g}$ to $\mathfrak{h}$; then it is a known result of Chevalley that the restriction

$$\chi: J^*(\mathfrak{g}) \to J^*(\mathfrak{h}) \tag{9.2.1}$$

of $\tilde{\chi}$ to $J^*(\mathfrak{g})$ defines an isomorphism of $J^*(\mathfrak{g})$ onto $J^*(\mathfrak{h})$. (See [3], § IV; also [12], Theorème 2, p. 19-10).

To prove the remaining part of Theorem 9.2 we shall need

LEMMA 9.2. *Let $I_j \in J^*(\mathfrak{g})$, $j = 1, 2, \cdots, l$, be given as in § 9.1. Let $x, y \in \mathfrak{h}$. Then x and y are conjugate with respect to W if and only if $I_j(x) = I_j(y)$ for $j = 1, 2, \cdots, l$.*

Proof. It is obvious from the definition of W that if x and y are conjugate with respect to W, $I_j(x) = I_j(y)$ for $j = 1, 2, \cdots, l$. Conversely, assume $I_j(x) = I_j(y)$, $j = 1, 2, \cdots, l$. Let $x_1, x_2, \cdots, x_{r_1}$ and $y_1, y_2, \cdots, y_{r_2}$ be, respectively, the distinct conjugates of x and y under W. Assume x is not conjugate to y. Then x_i, y_j, $i = 1, 2, \cdots, r_1$, $j = 1, 2, \cdots, r_2$, represent $r_1 + r_2$ points in $\mathfrak{h}$. Since points in $\mathfrak{h}$ are obviously algebraic varieties there exists $F \in S^*(\mathfrak{h})$ such that $F(x_i) = 0$, $i = 1, 2, \cdots, r_1$, $F(y_j) = 0$, $j = 2, \cdots, r_2$, and $F(y_1) = 1$. But then if

$$\tilde{F} = \sum_{\sigma \in W} \sigma(F),$$

it follows that $\tilde{F} \in J^*(\mathfrak{h})$, $\tilde{F}(y) \neq 0$ whereas $F(x) = 0$. But $\chi(I_j)$, $j = 1, 2, \cdots, l$, generate $J^*(\mathfrak{h})$ (see (9.2.1). Thus there exists j such that $I_j(x) \neq I_j(y)$. This is a contradiction. Q. E. D.

Proof of Theorem 9.2 *continued.* Assume $m = s$. Then $c^{p_j} = 1$ implies $j = l$ by Lemma 9.1. Thus we conclude $I_j(x) = 0$ for $j = 1, 2, \cdots, l-1$ and $I_l(x) \neq 0$.

Now it is well known (e.g. see [9], Theorem 6) that we may write $x = x_1 + x_2$, uniquely, where x_1 is semi-simple, x_2 is nilpotent and $[x_1, x_2] = 0$. By the uniqueness of this decomposition it is clear that $Ax_1 = cx_1$ and $Ax_2 = cx_2$. Furthermore, by hypothesis we know that $x_1 \neq 0$. Thus if we apply the previous argument to the relation $Ax_1 = cx_1$ it follows that $I_j(x_1) = 0$ for $j = 1, 2, \cdots, l-1$, and $I_l(x_1) \neq 0$.

Now since x_1 is semi-simple it lies in a Cartan subalgebra. Without loss of generality we may assume $x_1 \in \mathfrak{h}$. Now let γ be the Coxeter-Killing transformation given as in § 8.1. By Corollary 8.6, Theorem 7.3 and Theorem 6.7 there exists a cyclic vector $z \in \mathfrak{h}$ such that $\gamma z = \omega z$. If we apply the argument above once more to the relation $A_\gamma z = \omega z$, where A_γ is any extension of γ, it follows that $I_j(z) = 0$ for $j = 1, 2, \cdots, l-1$ and $I_l(z) \neq 0$. But then by Lemma 9.2, x_1 must be conjugate to a scalar multiple of z. Thus x_1 is cyclic. But then x_1 is regular. Since $[x_1, x_2] = 0$ this implies $x_2 \in \mathfrak{h}$. But x_2 is nilpotent. Hence $x_2 = 0$ or $x = x_1$. Thus x is cyclic.

Now since the regular vector $x \in \mathfrak{h}$ is an eigenvector of A it follows that $\mathfrak{h}$ is stable under A. Let $\tau \in W$ be the restriction of A to $\mathfrak{h}$. By Lemma 7.1 ω is an eigenvalue of τ. Let $y \in \mathfrak{h}$ be the corresponding eigenvector. The argument above applied to y proves that y is cyclic and when properly normalized there exists $\sigma \in W$ such that $\sigma z = y$. Now let $\gamma_1 = \sigma\gamma\sigma^{-1}$. Then γ_1 is a Coxeter-Killing transformation and $\gamma_1 y = \omega y$. But then $\tau^{-1}\gamma_1$ leaves y fixed. But it is well known that the only element of W which leaves a regular element fixed is the identity (see [8]). Thus τ is a Coxeter-Killing transformation and since A is an extension of τ, it follows from Theorem 8.6 that A is a principal element of G. Q. E. D.

Observe that Theorem 9.2 is a generalization of Corollary 8.6.

In [4] an important role is played by a regular eigenvectaor of γ. It is easy to see (see [4]) that the eigenvalue corresponding to any regular eigenvector of γ is a primitive s root of unity. By Theorem 9.2 we see that all such eigenvectors are cyclic.

Corollary 9.2 characterizes a Coxeter-Killing transformation among all elements in W.

COROLLARY 9.2. *Let $\sigma \in W$ be arbitrary and let c be an eigenvalue of σ.*

Then c is a primitive m-th root of unity, where m is an integer which divides m_j+1 for some exponent m_j of $\mathfrak{g}$. In particular $m \leqq s$. Moreover, if $m=s$, then σ is a Coxeter-Killing transformation and the eigenvector of σ corresponding to c is a cyclic element of $\mathfrak{g}$.

9.3. A corollary of the proof of Theorem 9.2 yields a characterization of cyclic elements in $\mathfrak{g}$.

COROLLARY 9.2. *Let I_j, $j=1,2,\cdots,l$, be the invariant polynomials on $\mathfrak{g}$ given as in* § 9.1. *Let $x \in \mathfrak{g}$. Then x is cyclic if and only if*

$$I_j(x)=0 \qquad \text{for } j=1,2,\cdots,l-1$$

and

$$I_l(x) \neq 0.$$

Proof. The proof that the equations above hold when x is cyclic has been given in the proof of Theorem 9.2. Assume, conversely, that these equations hold. Write

$$x = x_1 + x_2, \tag{9.3.1}$$

where x_1 is semi-simple, x_2 is nilpotent and $[x_1, x_2]=0$. (See [9], Theorem 6). By Theorem 9.1 $x_1 \neq 0$. Without loss of generality we may assume $x_1 \in \mathfrak{h}$. Consider $\mathfrak{g}^{x_1}$. It is clear that $\mathfrak{g}^{x_1}$ is generated linearly by $\mathfrak{h}$ and all root vectors e_ϕ, where $(\phi, x_1)=0$. It follows easily that $\mathfrak{g}^{x_1}=\mathfrak{c}+[\mathfrak{g}^{x_1},\mathfrak{g}^{x_1}]$ is a direct sum (see [9], Theorem 7), where $\mathfrak{c}$ is the center of $\mathfrak{g}^{x_1}$. Furthermore, $[\mathfrak{g}^{x_1},\mathfrak{g}^{x_1}]$ is semi-simple and $\mathfrak{c} \subseteq \mathfrak{h}$. Now $x_2 \in \mathfrak{g}^{x_1}$. Write $x_2 = y_1 + y_2$, where $y_1 \in \mathfrak{c}$ and $y_2 \in [\mathfrak{g}^{x_1},\mathfrak{g}^{x_1}]$. It follows immediately that y_2 is a nilpotent element of $[\mathfrak{g}^{x_1},\mathfrak{g}^{x_1}]$ and hence y_2 is a nilpotent element of $\mathfrak{g}$. (See footnote 3.)

But $x_1+y_1 \in \mathfrak{h}$ is semi-simple. Writing $x=(x_1+y_1)+y_2$ gives a second decomposition of the form (9.3.1). By uniqueness $y_1=0$ and hence $x_2 \in [\mathfrak{g}^{x_1},\mathfrak{g}^{x_1}]$. Applying Lemma 3.3 there exists $y \in [\mathfrak{g}^{x_1},\mathfrak{g}^{x_1}]$ such that $[y, x_2]=x_2$. Of course $[y, x_1]=0$. Thus if $A^\lambda = \operatorname{Exp} \lambda y$, it is clear that

$$A^\lambda x = x_1 + e^\lambda x_2.$$

But for any $F \in J^*(\mathfrak{g})$, $F(x)=F(A^\lambda x)$. By choosing λ such that e^λ is arbitrarily close to 0 it follows from continuity that $F(x)=F(x_1)$. In particular, $I_j(x_1)=0$ for $j=1,2,\cdots,l-1$ and $I_l(x_1)\neq 0$. But then as in the proof of Theorem 9.2 it follows that x_1 is cyclic. But then x_1 is regular and hence $[x_1,x_2]=0$ implies $x_2 \in \mathfrak{h}$. Since x_2 is nilpotent this implies $x_2=0$ and hence $x=x_1$ is cyclic. Q.E.D.

Even without knowledge of Corollary 9.2 it is interesting to observe that the conditions of that corollary, which singles out I_l, is independent of the set of generators I_j of $J^*(\mathfrak{g})$ so long as they are homogeneous, alge-

braically independent and ordered the way they are. This would not be necessarily true if I_j was singled out where $j < l$.

UNIVERSITY OF CALIFORNIA, BERKELEY.

REFERENCES.

[1] A. Borel, "Groupes linéaires algébriques," *Annals of Mathematics*, vol. 64 (1956), pp. 20-82.

[2] H. Cartan, "La transgression dans un group de Lie et dans un espace fibre principle," *Colloque de Topologie*, Bruxelles, 1950, pp. 57-71.

[3] C. Chevalley, "The Betti numbers of the exceptional simple Lie groups," *Proceedings of the International Congress of Mathematicians*, vol. II (1950), pp. 21-24.

[4] A. J. Coleman, "The Betti numbers of the simple Lie groups," *Canadian Journal of Mathematics*, vol. 10 (1958), pp. 349-356.

[5] H. S. M. Coxeter, "The product of the generators of a finite group generated by reflections," *Duke Mathematical Journal*, vol. 18 (1951), pp. 765-782.

[6] E. B. Dynkin, "Some properties of the system of weights of a linear transformation of a semisimple Lie group," *Doklady Akademii Nauk SSSR (N. S.)*, vol. 71 (1950), pp. 221-224 (Russian).

[7] ———, "Semisimple subalgebras of semisimple Lie algebras," *American Mathematical Society Translations*, vol. 6 (1957), pp. 111-244.

[8] F. Gantmacher, "Canonical representation of automorphisms of a complex semisimple Lie group," *Matematiceski Sbornik*, vol. 47 (1939), pp. 101-146.

[9] N. Jacobson, "Completely reducible Lie algebras of linear transformations," *Proceedings of the American Mathematical Society*, vol. 2 (1951), pp. 105-133.

[10] A. I. Mal'cev, "On semi-simple subgroups of Lie groups," *American Mathematical Society Translations*, no. 33 (1950).

[11] V. V. Morosov, "On a nilpotent element of a semi-simple Lie algebra," *Akademiia Nauk SSSR (Doklady)*, vol. 36 (1942), pp. 83-86.

[12] Séminaire Sophus Lie, le année 1954/1955, *Théorie des algèbre de Lie, Topologie des groupes de Lie*, Ecole Normale Supérieure, Paris, 1955.

[13] J. de Siebenthal, "Sur certaines sous-groupes de rang un des groupes de Lie clos," *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, vol. 230 (1950), pp. 910-912.

[14] H. Weyl, *The structure and representation of continuous groups*, Institute for Advanced Study notes by R. Brauer, 1934-1935, reprinted 1955.

(*Added in proof:* The empirical procedure for determining the exponents of $\mathfrak{g}$, discovered by A. Shapiro, was recently found independently by R. Steinberg who likewise speaks about the lack of any proof for the procedure. See § 9 in

[15] R. Steinberg, "Finite reflection groups," *Transactions of the American Mathematical Society*, vol. 91 (1959), pp. 493-504.

As we have noted in the Introduction a proof (see Corollary 8.7) of the procedure is a consequence of our main results. The paper [15] is mainly devoted to giving a proof of two empirical discoveries of H. S. M. Coxeter. A proof of these discoveries is also given here (see Theorem 8.4)).

ON THE CONNECTEDNESS THEOREM IN ALGEBRAIC GEOMETRY.*[1]

By Wei-Liang Chow.

To Zariski on his 60th birthday.

1. Introduction. The Connectedness Theorem in abstract algebraic geometry was first formulated and proved by Zariski [14]; it stems from his attempt to prove the Principle of Degeneration over an abstract field and actually contains that principle as a special case. The proof of Zariski makes extensive use of his theory of holomorphic functions on an algebraic variety; in fact, this latter theory was developed by him specially for this purpose, and, as has been pointed out by Zariski himself, it has in a sense the Connectedness Theorem as its principal application. In view of the fundamental importance of the Connectedness Theorem on the one hand and the very complicated nature of Zariski's theory of holomorphic functions on the other, it is clearly very desirable to have for this theorem a proof of a simpler and more elemetnary nature. Furthermore, in consonance with the recent tendencies in algebraic geometry toward increasing arithmetic applications, one would naturally wish to generalize this theorem to the case of a correspondence between the rational transforms of arbitrary local domains (the exact meaning of this statement will be explained later in § 2). In a recent paper [4] we have given a very simple proof of such a generalization for a special case of the theorem, namely the Principle of Degeneration. In the present paper we shall solve the problem completely by giving a simple proof of the Connectedness Theorem in just about as general a version as we know how to formulate it at this stage of the subject.

Let R be a Noetherian domain with the quotient field K, and let S^n be the projective space of dimension n in the algebraic geometry over a universal domain $\mathfrak{K}$ which contains the field K. Let $\mathfrak{p}$ be a prime ideal in R, and denote by $\bar{R}$ the residue field $R/\mathfrak{p}$ of R over $\mathfrak{p}$; generally for any element x in R or a polynomial $f(Y)$ in $R[Y]=R[Y_0, Y_1, \cdots, Y_m]$, where the Y_i are indeterminates, we shall denote by $\bar{x}$ or $\bar{f}(X)$ respectively the corresponding element

* Received April 28, 1958; revised August 28, 1959.

[1] This work was partially supported by a research grant of the National Science Foundation.

in $\bar{R}$ or polynomial in $\bar{R}[Y]$ under the canonical homomorphism of R onto $\bar{R}$. We shall denote by $\bar{S}^n$ the projective space of dimension n in the algebraic geometry over a universal domain Λ which contains the field $\bar{R}$. Let Z be a positive r-cycle in S^n such that its associated point $y=(y_0, y_1, \cdots, y_m)$ in S^m is rational over K. A point η in $\bar{S}^m$ is said to be a *specialization* of the point y at the prime ideal $\mathfrak{p}$ if whenever a form $f(Y)$ satisfies the condition $f(y)=0$, it satisfies also the condition $\bar{f}(\eta)=0$. Since the condition for a point to be an associated point is "universal," every specialization η of y at $\mathfrak{p}$ is the associated point of a positive r-cycle $Z(\eta)$ in $\bar{S}^n$, of the same degree as Z; we shall say that the cycle $Z(\eta)$ is a *specialization* of the cycle Z at $\mathfrak{p}$ or at $R_{\mathfrak{p}}$, where $R_{\mathfrak{p}}$ is the quotient ring of R with respect to $\mathfrak{p}$. It is easily seen that the set of all specializations of y at $\mathfrak{p}$ is an $\bar{R}$-closed subset in $\bar{S}^m$, and it follows from this that the union of the supports of all specializations of Z at $\mathfrak{p}$ is also an $\bar{R}$-closed subset in $\bar{S}^n$. Recalling the definition that R is *analytically irreducible* at $\mathfrak{p}$ if the completion of the local ring $R_{\mathfrak{p}}$ is an integral domain, we can state the Connectedness Theorem as follows:

Let R be a Noetherian domain with the quotient field K, and let Z be a rational positive cycle over K in S^n; if Z is connected and if $\mathfrak{p}$ is a prime ideal in R such that R is analytically irreducible at $\mathfrak{p}$, then union of the supports of all the specializations of Z at $\mathfrak{p}$ is also connected.

Apart from the extension to an arbitrary Noetherian domain (instead of the coordinate ring of an algebraic variety), the above version of the Connectedness Theorem coincides in substance with the original formulation of Zariski. Now, since the Connectedness Theorem concerns itself essentially with the properties of a cycle Z with respect to a prime ideal $\mathfrak{p}$ in R, there will be no loss of generality if we replace the ring R by the quotient ring $R_{\mathfrak{p}}$, so that we can assume from the beginning that R is already a local domain. Moreover, since the concept of analytic irreducibility involves the completion of R, we may just as well assume further that R is itself a complete local domain. It turns out that, once put in this strictly local form, the Connectedness Theorem can be generalized to a theorem in the "relative" geometry, in a similar way as we have generalized the Principle of Degeneration in [4]. This generalization, which we shall call the General Connectedness Theorem, can be stated as follows:

GENERAL CONNECTEDNESS THEOREM. *Let R be a complete local domain with the quotient field K and the residue field $\bar{R}$, and let Z be a rational positive cycle over K in S^n; if Z is K-connected, then the union of the supports of all the specializations of Z at R is $\bar{R}$-connected.*

We remark that here the topological concepts such as "closed," "connected," etc., refer to the well-known Zariski topology, in which the closed subsets are unions of finite number of algebraic varieties, and the relative topological concepts such as "K-closed," "K-connected," etc., refer to the relative Zariski topology, in which the closed subsets are unions of finite number of complete sets of conjugate varieties over K. The use of these topological terminology, though not really necessary, proves to be very convenient. Although it is really only a trivial observation, we should like to point out in this connection that our formulation of the General Connectedness Theorem does not at all imply that the preservation of connectedness under specialization, which holds in the absolute Zariski topology, holds also in the relative Zariski topology over a *given* ground field; on the contrary, a little reflection shows that it is rather the disconnectedness over a ground field that is preserved under a specialization over the same ground field.

The General Connectedness Theorem contains two special cases: The Special Connectedness Theorem, where the cycle Z consists of a single point, so that we are dealing essentially with what corresponds to a birational transformation in the geometric case, and the Principle of Degeneration, where the local domain R is a real discrete valuation ring, so that there is a uniquely determined specialization of Z at R. Conversely, once we have proved these two special cases, we can easily obtain from them the Connectedness Theorem, as we shall show later in section 4. However, in order to prove the General Connectedness Theorem in its full generality as formulated above, we need something more than a simple combination of these two special cases. The reason for this is not difficult to see. For the hypothesis of the General Connectedness Theorem provides only the relative connectedness of the cycle Z over the complete local domain R, while the application of the Principle of Degeneration (in the form formulated in [4]) presupposes that we have some information about the relative connectedness of Z over some complete real discrete valuation ring dominating R, and it is clear that the relative connectedness of a cycle is in general not preserved under such an extension. In order to fill this gap, we need a result which says essentially that if a cycle Z splits into two disconnected parts over every complete real discrete valuation ring dominating R and this is in "continuous" manner, then Z cannot be connected over R. It turns out that these considerations lead us in a natural way to a refinement of the General Connectedness Theorem, which we shall call (for reasons which will be apparent) the Extended Principle of Degeneration. We shall prove this Extended Principle of Degeneration only for the case of a complete regular local ring; whether this Extend Principle

holds for the general case of an arbitrary complete local domain, is a question which will not be settled here, although it seems very likely that the answer to it is in the affirmative. However, so far as the General Connectedness Theorem is concerned, this restriction to regular local rings is not a serious point, for a very simple argument (in section 4) shows that the validity of this theorem for a regular local ring implies its validity in the general case. On the other hand, this restriction to regular local rings enables us to obtain, in case of the Special Connectedness Theorem, yet another refinement, which is not generally true without this restriction. We shall say that a point set is *linearly connected* if every two points in the set can be connected by a sequence of rational curves in the set. Then we can prove that in the Special Connectedness Theorem for a regular local ring the set of all specializations is not only connected, but also linearly connected. This stronger result, which we shall call the Linear Connectedness Theorem, is of fundamental importance for the theory of rational equivalence, as we shall show in our forthcoming work on the intersection theory of cycles and equivalence classes of cycles.

Our paper therefore consists of two main results, the Linear Connectedness Theorem and the Extended Principle of Degeneration; the former will be proved in section 3 and the latter will be proved in section 5. Our proof of the Linear Connectedness Theorem is based on an analysis of the properties of the quadratic transforms of a regular local ring, and we shall use in course of the proof some of the well-known results on this subject. Looked upon from this point of view, our proof is related to the recent proofs of Zariski [15] and Murre [10] of the Special Connectedness Theorem for a simple point in the geometric case. On the other hand, our proof of the Extended Principle of Degeneration is of a quite different nature; although the quadratic transforms play also an essential role in this proof, the main idea lies in a different direction and is essentially a generalization of the method used in our proof of the Principle of Degeneration in [4], which centers on the idea of Hensel's Lemma. Only, as we have to deal now with an entire system of specialization cycles at the center, instead of a single cycle, the elementary "resultant" method used in [4] proves to be too cumbersome and rather inadequate; instead, we shall draw more heavily on the theory of local rings, with the result that we are able not only to prove the more general result, but also to gain a better insight into the nature of the problem. Incidentally, we should like to point out that the result in [4] is not used in our present proof, which in this sense can be said to start from the beginning, while on the other hand our recent result on the Local Bertini Theorem [5] plays an essential role in the important process of reduction to the case of dimension 2.

As to terminology, we shall use here some of the terms in Weil's well-known *Foundations of Algebraic Geometry,* such as the terms "universal domain," "variables," "indeterminates," "cycles," etc., which have now become more or less standard; however, we shall not make use of any results in this book, so that a knowledge of it is not at all necessary for the understanding of the present paper. On the other hand, we shall assume that the reader is familiar with the theory of local rings, which is fundamental for our subject; we shall therefore use freely the basic notions and results in this theory, although we endeavor to give explicit references for all results beyond the very elementary ones. We shall also use for convenience the topological concepts based on the Zariski topology, either absolute or relative to a given ground field; the Zariski topology for algebraic varieties is of course involved right at the beginning already in the formulation of our problem, but later we shall introduce it also for sets of algebraic cycles as well as for sets of valuation rings dominating given local domains. Finally, in the last two sections we shall assume some knowledge of the theory of associated forms; it is sufficient for this purpose to know the properties of the associated forms listed at the beginning of § 4 in our paper [4].

2. Rational transforms. We begin by making a few remarks concerning the projective space S^n (or S^m) introduced in the preceding section. Although it is quite possible for us to work within a given universal domain provided we choose it suitably to include all the local rings we shall need in the course of our theory, it is nevertheless more convenient and probably in a sense also more appropriate to consider S^n as the "universal projective space" which can be defined as the logical union of all the projective spaces of dimension n over all possible universal domains. We remark however that we shall never invoke more than a finite number of universal domains at one time, so that we are not really involved in any of the logical difficulties usually connected with the use of the expression "all" in such a context. Without any reference to any universal domains, we can define the *universal projective space* S^n by the stipulations that any ordered system of $n+1$ elements $(z_0, z_1, \cdots, z_n)$ in any field (or integral domain), not all zero, defines a point z in S^n, and that two such systems define the same point in S^n if and only if their elements are contained in some one field and are proportional to each other in this field; the elements z_j are called the (homogeneous) coordinates of the point z. We shall say that the point z is rational over a field K if the ratios of its coordinates z_j are contained in K; when this is the case, we shall always assume (unless stated to the contrary) that the pro-

portionality factor has already been so chosen that the coordinates of z are all in K. In applying the usual algebro-geometrical operations to the entities in this universal projective space S^n we must of course see to it that the entities involved all belong to some one field, while among the entities belonging to different fields only very restricted types of relations can occur.

On the other hand, the projective space $\bar{S}^n$ remains, as it was before, to be the one over a given universal domain Λ, so that we can now consider $\bar{S}^n$ to be contained in the universal projective space S^n. However, this space $\bar{S}^n$ is in a sense the center of our attention, and we shall relate to it various entities in S^n in the following way. We shall say that a local ring $(R, \mathfrak{p})$ is *attached* to Λ if its residue field $\bar{R} = R/\mathfrak{p}$ is identified with a field contained in Λ, whereby the expression "a field in Λ" is to be understood in the sense of Weil's *Foundations* (i. e. Λ has infinite degree of transcendency over $\bar{R}$); the so defined concept of an attached local ring is somewhat more specific than that of a local ring by itself, for two local rings which are isomorphic but attached to distinct fields in Λ are to be considered here as different. *In this paper all the local rings are assumed to be attached to* Λ *in some ways,* so that we shall not always explicitly mention this fact. Furthermore, if a local ring $(R_1, \mathfrak{p}_1)$ contains R such that $R \cap \mathfrak{p}_1 = \mathfrak{p}$, and if R_1 is attached to Λ in such a way that the canonical embedding of $R/\mathfrak{p}$ into $R_1/\mathfrak{p}_1$ as abstract fields is accompanied by a corresponding embedding of the attached residue field of R in Λ into the attached residue field of R_1 in Λ, then we shall say that R_1 *dominates* R. In particular, we shall always assume that the completion R^* of R is attached to Λ in such a way that R^* dominates R, so that they have the same residue field in Λ. Once a local ring R is attached to Λ, the canonical homomorphism of R onto $\bar{R}$ will induce (under certain circumstances) a relation between those geometrical entities in S^n which are defined by means of R and similar entities in $\bar{S}^n$, such as the concept of a specialization of a cycle at $\mathfrak{p}$ described in the preceding section. For the sake of completeness and clarity, we shall begin here anew and repeat all the definitions.

Let $(R, \mathfrak{p})$ be a local domain of dimension t (attached to Λ), with the quotient field K and the residue field $\bar{R}$; for any element a in R or a polynomial $f(Y)$ in $R[Y] = R[Y_0, Y_1, \cdots, Y_m]$, we shall denote by $\bar{a}$ or $\bar{f}(X)$ respectively the corresponding element in $\bar{R}$ or polynomial in $\bar{R}[Y]$ under the canonical homomorphism of R onto $\bar{R}$. Let $y = (y_0, y_1, \cdots, y_m)$ be a point in S^m with coordinates in a field containing K; a point $\eta = (\eta_0, \eta_1, \cdots, \eta_m)$ in $\bar{S}^m$ is said to be a *specialization of y at R*, if for every form $f(Y)$ in $R[Y]$ the relation $f(y) = 0$ implies the relation $\bar{f}(\eta) = 0$. We shall denote by $\bar{y}(R)$ the set of all specializations of y at R, and it is easily seen that $\bar{y}(R)$

is an $\bar{R}$-closed subset in $\bar{S}^m$. If $(R_1, \mathfrak{p}_1)$ is a local domain which dominates $(R, \mathfrak{p})$ and if y is a point which is rational over a field containing R_1, then every specialization of y at R_1 is also a specialization of y at R, so that $\bar{y}(R_1)$ is contained in $\bar{y}(R)$. In case y is the associated point of a positive r-cycle Z in S^n, then every specialization of y at R is also the associated point of a positive r-cycle in $\bar{S}^n$, which we shall call a *specialization of* Z *at* R; we shall denote by $\bar{Z}(R)$ the set of all specializations of Z at R and denote by $|\bar{Z}(R)|$ the union of the supports of all the cycles in $\bar{Z}(R)$, and we observe that $|\bar{Z}(R)|$ is an $\bar{R}$-closed subset in $\bar{S}^n$.

We shall be particularly interested in the case where the point y is rational over K, and we shall say in this case that the point y defines a *rational transform* $y(R)$ of the local domain R; as we shall see, this notion of a rational transform of a local domain plays a fundamental role in our theory. The set $\bar{y}(R)$ is then called the *center* of the rational transform $y(R)$. If η is any point in $\bar{y}(R)$, consider the subring $\mathfrak{Q}(y(R)/\eta)$ in K consisting of all the elements of the form $f(y)/g(y)$, where $f(Y)$ and $g(Y)$ are forms of the same degree in $R[Y]$ and $\bar{g}(\eta) \neq 0$; it is easily seen that $\mathfrak{Q}(y(R)/\eta)$ is a local domain with the quotient field K, and that its maximal prime ideal $\mathfrak{p}(y(R)/\eta)$ consists of all the elements $f(y)/g(y)$ with $\bar{f}(\eta) = 0$. Since the residue field of $\mathfrak{Q}(y(R)/\eta)$ is isomorphic to the field $\bar{R}(\eta)$ in Λ, we shall attach $\mathfrak{Q}(y(R)/\eta)$ to Λ by identifying the residue field of $\mathfrak{Q}(y(R)/\eta)$ with $\bar{R}(\eta)$, and we shall call the so attached local domain $\mathfrak{Q}(y(R)/\eta)$ the *specialization ring* of the rational transform $y(R)$ at η. We observe that $\mathfrak{Q}(y(R)/\eta)$ evidently dominates the local domain R, and that if $\eta_j \neq 0$ for any one j, then $\mathfrak{Q}(y(R)/\eta)$ contains also the ring $R[y_0/y_j, \cdots, y_m/y_j]$; furthermore, it is easily seen that $\bar{y}(Q(y(R)/\eta))$ is the $\bar{R}$-variety in $\bar{S}^{m-1}$ consisting of all the specializations of η over $\bar{R}$. The point η is said to be *normal* or *simple* in the rational transform $y(R)$ if $\mathfrak{Q}(y(R)/\eta)$ is integrally closed or regular respectively, and when such is the case, we shall also say that the rational transform $y(R)$ is normal or simple at η respectively. We shall say that the rational transform $y(R)$ is normal or non-singular if it is normal or simple respectively at every point in its center $\bar{y}(R)$.

The concept of a rational transform $y(R)$ of a local domain R is a natural generalization of the concept of a rational transformation T of an algebraic variety V around a given point p of the variety. It belongs to the local geometry in the strict sense that one is concerned with what corresponds to the behavior of the rational transformation T in the infinitesimal neighborhood of p in V, not a finite neighborhood, however small. For this reason the only points on our rational transform $y(R)$ are the points in the center $\bar{y}(R)$, which

corresponds in the geometric case to the total image $T(p)$ of the point p under T. However, we should like to stress here that we are really considering the points in $\bar{y}(R)$ not as points in what corresponds to the image variety $T(V)$ of V, but rather as points in what corresponds to the graph of T in the product space $V \times T(V)$, so that $\bar{y}(R)$ should be considered as corresponding to $p \times T(p)$, not to $T(p)$; for our definition of the specialization ring $\mathfrak{Q}(y(R)/\eta)$ at a point η in $\bar{y}(R)$ corresponds to the specialization ring of the graph of T at a point in $p \times T(p)$, not that of $T(V)$ at a point of $T(p)$. The reason for introducing here what corresponds to the graph rather than the image is quite easily understood, for the graph of a rational transformation contains essentially the complete information about the transformation, while the image is merely its projection on one of the factor spaces and hence its introduction is often not necessary, as is the case in our present studies.

The study of rational transforms is of fundamental importance not only for our present purpose, but also for many other problems in abstract local geometry. In this section, we shall limit ourselves to stating and proving a few basic properties of these transforms, which we shall need later. The discerning reader will notice that most of these are merely generalizations to arbitrary local domains of some of the elementary properties given in [11] for the geometric case, and it is therefore not surprising that we have also taken over some of the proofs from that paper.

LEMMA 2.1. *If $y(R)$ is a rational transform of R, then for any two points η and η' in $\bar{y}(R)$, $\mathfrak{Q}(y(R)/\eta)$ contains $\mathfrak{Q}(y(R)/\eta')$ if and only if η' is a specialization of η over $\bar{R}$.*

Proof. The condition is evidently sufficient. To prove the necessity, let $g(Y)$ be any form in $R[Y]$ such that $\bar{g}(\eta') \neq 0$, and let $f(Y)$ be a form in $R[Y]$ of the same degree as $g(Y)$ such that $\bar{f}(\eta) \neq 0$; if $\mathfrak{Q}(y(R)/\eta)$ contains $\mathfrak{Q}(y(R)/\eta')$, then $f(y)/g(y)$ being an element in $\mathfrak{Q}(y(R)/\eta')$ must be contained in $\mathfrak{Q}(y(R)/\eta)$. Since $\bar{f}(\eta) \neq 0$, this implies that $\bar{g}(\eta) \neq 0$. Since this is true for any form $g(Y)$ in $R[Y]$ and since any form in $\bar{R}[Y]$ can be obtained as a form $\bar{g}(Y)$, this shows that η' is a specialization of η over $\bar{R}$.

In the special case when the local domain R is a valuation ring, the center $\bar{y}(R)$ of any rational transform $y(R)$ of R consists of a single point; in fact, there exists in this case some one y_j such that $y_0/y_j, \cdots, y_m/y_j$ are all contained in R, and the point $(\overline{y_0/y_j}, \cdots, \overline{y_m/y_j})$ is evidently the only specialization of y at R. Furthermore, it is easily seen from the well-known maximality properties of a valuation ring that in this case we have $\mathfrak{Q}(y(R)/\bar{y}(R)) = R$.

In the general case of an arbitrary local domain R, we consider a valuation ring M in K dominating R; then, for any rational transform $y(R)$ of R, the point $\bar{y}(M)$ is evidently contained in $\bar{y}(R)$. We shall call this point $\bar{y}(M)$ the *center* of M in the rational transform $y(R)$. We maintain that M dominates $\mathfrak{Q}(y(R)/\bar{y}(M))$. To see this, let y_j be so chosen that the elements $y_0/y_j, \cdots, y_m/y_j$ are all in M and hence $\bar{y}(M) = (\overline{y_0/y_j}, \cdots, \overline{y_m/y_j})$; if $f(Y)$ is any form of degree d in $R[Y]$, then $f(y)/y_j{}^d$ is an element in M, and since M dominates R, it is a non-unit in M if and only if $\bar{f}(\bar{y}(M)) = 0$. It follows easily from this that any element $f(y)/g(y) = (f(y)/y_j{}^d)/(g(y)/y_j{}^d)$ in $\mathfrak{Q}(y(R)/\bar{y}(M))$ is an element in M, and that it is a non-unit in M if and only if it is such in $\mathfrak{Q}(y(R)/\bar{y}(M))$. This result, together with Lemma 2.1, gives us almost immediately the following lemma.

LEMMA 2.2. *Let $y(R)$ be a rational transform of a local domain R, let M be a valuation ring in K which dominates R, and let η be a point in $\bar{y}(R)$; then $\bar{y}(M) = \eta$ if and only if M dominates $\mathfrak{Q}(y(R)/\eta)$.*

It is well-known that any local ring in a field K is dominated by some valuation ring in K. Applying this to the local ring $\mathfrak{Q}(y(R)/\eta)$, we conclude from Lemma 2.2 that given any point η in $\bar{y}(R)$ there exists a valuation ring M in K dominating R such that $\eta = \bar{y}(M)$. If we denote by $\mathfrak{V}(R)$ the *set of all valuation rings in K dominating R*, then the correspondence $M \to \bar{y}(M)$ defines a mapping $\mathfrak{V}(R)$ *onto* the center $\bar{y}(R)$ of $y(R)$. We now introduce a topology in $\mathfrak{V}(R)$, called its *Zariski topology*, by the stipulation that a subset in $\mathfrak{V}(R)$ is said to be closed if it is the inverse image under this mapping of a closed subset in $\bar{y}(R)$ for some one rational transform $y(R)$ of R, whereby $\bar{y}(R)$ is understood to be endowed with its Zariski topology (induced by the Zariski topology in $\bar{S}^m$). If we consider only the Zariski $\bar{R}$-topology of $\bar{y}(R)$ for every $y(R)$, then we obtain the $\bar{R}$-topology of $\mathfrak{V}(R)$, and we have therefore such notions as $\bar{R}$-closed, $\bar{R}$-connected, etc. That this definition of a closed subset in $\mathfrak{V}(R)$ actually defines a topology in $\mathfrak{V}(R)$ can be easily verified. We observe also that this topology is the least fine among all topologies in $\mathfrak{V}(R)$ for which the mapping $M \to \bar{y}(M)$ is continuous for every rational transform $y(R)$ of R, both in the absolute case and in the relative case.

In case y is the associated point of a positive cycle Z in S^n, then for every valuation ring M in K dominating R we have a specialization cycle $\bar{Z}(M)$ of Z at R, and in this way we can obtain all specializations of Z at R, so that we can set $\bar{Z}(R) = \{\bar{Z}(M) \mid M \in \mathfrak{V}(R)\}$. If $F(U)$ is the associated form of the cycle Z, then we shall denote the associated form of the

specialization cycle $\bar{Z}(M)$ by $\bar{F}_M(U)$. We note that both forms $F(U)$ and $\bar{F}_M(U)$ are defined only up to proportionality factors in K and $\bar{M}$ respectively, and that even when $F(U)$ is taken to be a form in $M[U]$, $\bar{F}_M(U)$ is not necessarily the residue image of $F(U)$ in $\bar{M}[U]$; in order to get $\bar{F}_M(U)$ as the residue form of $F(U)$, one has to normalize $F(U)$ by dividing it by one of its coefficients which have the lowest value under the valuation of M, so that all coefficients in $F(U)$ be in M but not all non-units.

Let $z = (z_0, z_1, \cdots, z_l)$ be a point in S^l which is rational over K, and consider the rational transform $z(R)$; then we can define a birational correspondence T between the two rational transforms $y(R)$ and $z(R)$ as follows: Two points η and ζ in $\bar{y}(R)$ and $\bar{z}(R)$ respectively are said to correspond to each other under T if there exists a valuation ring M in K dominating R such that $\eta = \bar{y}(M)$ and $\zeta = \bar{z}(M)$. In order to avoid possible ambiguities, we shall consider the correspondence T as from $y(R)$ to $z(R)$, so that the inverse correspondence from $z(R)$ to $y(R)$ will be denoted by T^{-1}; if η or ζ is any point in $\bar{y}(R)$ or $\bar{z}(R)$ respectively, then we shall denote by $T(\eta)$ or $T^{-1}(\zeta)$ respectively the set of all points in $\bar{z}(R)$ or $\bar{y}(R)$ which correspond to η or ζ under T or T^{-1} respectively. As the reader will readily perceive, this definition of a birational correspondence is essentially the same as that given in [11]. We shall say that the birational correspondence T is *regular* at a point η in $\bar{y}(R)$, if there exists a point ζ in $\bar{z}(R)$ corresponding to η under T such that $\mathfrak{Q}(y(R)/\eta)$ contains $\mathfrak{Q}(z(R)/\zeta)$. Finally, we introduce the *join* $y \circ z$ of the two points y and z, which is defined as the point in $S^{(m+1)(l+1)-1}$ whose coordinates are the elements $y_i z_j$, for $i = 0, 1, \cdots, m$, and $j = 0, 1, \cdots, l$, arranged in some arbitrary (but fixed) order; the rational transform $y \circ z(R)$ is then said to be the *join* of the rational transforms $y(R)$ and $z(R)$. It is clear that if M is any valuation ring in K dominating R, then we have the relation $\overline{y \circ z}(M) = \bar{y}(M) \circ \bar{z}(M)$; it follows easily from this that the birational correspondence between $y \circ z(R)$ and $y(R)$ is regular at every point in $\overline{y \circ z}(R)$.

LEMMA 2.3. *If the birational correspondence T between $y(R)$ and $z(R)$ is regular at a point η in $y(R)$, then $T(\eta)$ consists of exactly one point.*

Proof. By definition there exist a point ζ in $\bar{z}(R)$ and a valuation ring M in K dominating R such that $\eta = \bar{y}(M)$, $\zeta = \bar{z}(M)$, and $\mathfrak{Q}(y(R)/\eta) \supset \mathfrak{Q}(z(R)/\zeta)$. According to Lemma 2.2, M dominates both $\mathfrak{Q}(y(R)/\eta)$ and $\mathfrak{Q}(z(R)/\zeta)$; it follows that $\mathfrak{Q}(y(R)/\eta)$ dominates $\mathfrak{Q}(z(R)/\zeta)$. If M_1 is any valuation ring in K dominating $\mathfrak{Q}(y(R)/\eta)$, then it must also dominate $\mathfrak{Q}(z(R)/\zeta)$; it follows then by Lemma 2.2 again that $\bar{z}(M_1) = \zeta$, which proves our lemma.

LEMMA 2.4. *If $y(R)$ is normal at a point η and if $T(\eta)$ consists of a finite number of points, then T is regular at η.*

Proof. It is easily seen that, without affecting the validity of our lemma, we can replace $z(R)$ by another rational transform of R which is in biregular correspondence with it; in particular, we can replace $z(R)$ by the rational transform defined by a point whose coordinates are the monomials of the elements $z_0, z_1, \cdots, z_l$ of a given degree, arranged in some arbitrary order. By making such a replacement of $z(R)$ if necessary, we can therefore obtain that if $\zeta^{(1)}, \cdots, \zeta^{(d)}$ are the points contained in $T(\eta)$, then none of the coordinates ${\zeta^{(1)}}_0, \cdots, {\zeta^{(d)}}_0$ vanishes. Then $\mathfrak{Q}(z(R)/\zeta^{(i)})$ contains the ring $R[z_1/z_0, \cdots, z_l/z_0]$ for every $i = 1, \cdots, d$, and is in fact the quotient ring of $R[z_1/z_0, \cdots, z_l/z_0]$ with respect to the ideal

$$\mathfrak{q}_i = \mathfrak{p}(z(R)/\zeta^{(i)}) \cap R[z_1/z_0, \cdots, z_l/z_0].$$

Since each $\mathfrak{Q}(z(R)/\zeta^{(i)})$ is contained in some one valuation ring in $\mathfrak{V}(\mathfrak{Q}(y(R)/\eta))$, it follows that $R[z_1/z_0, \cdots, z_l/z_0]$ is contained in the intersection of all valuation rings in $\mathfrak{V}(\mathfrak{Q}(y(R)/\eta))$. Since $y(R)$ is normal at η, $\mathfrak{Q}(y(R)/\eta)$ coincides with the intersection of all valuation rings in $\mathfrak{V}(\mathfrak{Q}(y(R)/\eta))$ and hence contains $R[z_1/z_0, \cdots, z_l/z_0]$. Since $\mathfrak{q}_i$ is the restriction to $R[z_1/z_0, \cdots, z_l/z_0]$ of the maximal ideal in some one valuation ring in $\mathfrak{V}(\mathfrak{Q}(y(R)/\eta))$, it must contain the ideal

$$\mathfrak{q} = \mathfrak{p}(y(R)/\eta) \cap R[z_1/z_0, \cdots, z_l/z_0],$$

and since $\mathfrak{Q}(y(R)/\eta)$ contain the quotient ring of $R[z_1/z_0, \cdots, z_l/z_0]$ with respect to $\mathfrak{q}$, it must also contain $\mathfrak{Q}(z(R)/\zeta^{(i)})$. This shows that T is regular at the point η.

We make a digresion here to observe that up to now we have not used at all the crucial property of a local domain, that it is Noetherian; in fact, all our definitions (except for the definition of a simple point) and results up to now hold for any (commutative) integrity domain with the property that the set of all non-units is an ideal, i. e., what is sometimes called a quasi-local domain. While any deeper study of the rational transforms must of course involve the Noetherian or other similar properties, it is nevertheless convenient to avail ourselves of the fact that some of the elementary notions and results hold for the more general case. This is the justification for stating Lemma 2.2 above for any arbitrary valuation ring M, without the Noetherian restriction. In this paper we shall only consider rational transforms of (Noetherian) local domains; however; in considering the valuation rings dominating a local domain, we shall not restrict ourselves to the

Noetherian ones. Although it is possible in principle to get along without using any other valuation rings except those which are discrete and of rank 1, as shown by Lemma 2.7 below, it is very desirable to be able to use others whenever it turns out to be convenient to do so. We shall meet later occasions when it is convenient to use discrete valuation rings of rank 2.

From now on the Noetherian property of the local domain R will play an essential role. We observe first that by virtue of this Noetherian property the local domain R has a finite dimension t, which can be defined either as the rank of the maximal prime ideal $\mathfrak{p}$ or the number of elements in a system of parameters.

LEMMA 2.5. *If $y(R)$ is a rational transform of a local domain of dimension t, then any point in $\bar{y}(R)$ has a dimension at most $t-1$ over $\bar{R}$, so that the maximum dimension of the algebraic set $\bar{y}(R)$ is at most $t-1$.*

Proof. Let η be any point in $\bar{y}(R)$, and let M be a valuation ring in K dominating $\mathfrak{Q}(y(R)/\eta)$. According to [2], Theorem 1, the residue field of M has a dimension at most $t-1$ over $\bar{R}$; hence the residue field $\bar{R}(\eta)$ of $\mathfrak{Q}(y(R)/\eta)$ can have a dimension at most $t-1$ over $\bar{R}$, which shows that η has a dimension at most $t-1$ over $\bar{R}$.

LEMMA 2.6. *Let $y(R)$ be a rational transform of a local domain of dimension t; if a point η in $\bar{y}(R)$ has the dimension $t-1$ over $\bar{R}$, then there are only a finite number of valuation rings in K which dominate $\mathfrak{Q}(y(R)/\eta)$, and these valuation rings are real discrete (i.e. regular local domains of dimension 1).*

Proof. Since the residue field $\bar{R}(\eta)$ of $\mathfrak{Q}(y(R)/\eta)$ has the dimension $t-1$ over $\bar{R}$, the dimension of $\mathfrak{Q}(y(R)/\eta)$ must be 1; for, if the dimension of $\mathfrak{Q}(y(R)/\eta)$ were greater than 1, then there would exist a valuation ring in K dominating $\mathfrak{Q}(y(R)/\eta)$ whose residue field has a positive dimension over $\bar{R}(\eta)$ and hence a dimension greater than $t-1$ over $\bar{R}$, in contradiction to [2], Theorem 1. According to [7], the integral closure R_1 of $\mathfrak{Q}(y(R)/\eta)$ is Noetherian and hence the ideal $R_1\mathfrak{p}(y(R)/\eta)$ has only a finite number of (minimal) prime divisors; furthermore, the quotient ring of R_1 with respect to any one of these prime divisors is a real discrete valuation ring whose residue field is a finite algebraic extension of $\bar{R}(\eta)$. Since any valuation ring in K dominating $\mathfrak{Q}(y(R)/\eta)$ must coincide with one of these quotient rings, our lemma follows if we observe in addition that since the residue field of such a valuation ring is a finite algebraic extension of $\bar{R}(\eta)$, there are only a finite number of possible ways to embed it as a field extension of $\bar{R}(\eta)$ in Λ.

LEMMA 2.7. *Let $y(R)$ be a rational transform of an unmixed ($=$ equi-dimensional) local domain of dimension t, and let η be any point in $y(R)$; then there exists a real discrete valuation ring in K which dominates $\mathfrak{Q}(y(R)/\eta)$ and whose residue field has the dimension $t-1$ over $\bar{R}$.*

Proof. Without the last condition on the dimension over R this lemma holds for any arbitrary local domain R (not necessarily unmixed); one has only to apply to $\mathfrak{Q}(y(R)/\eta)$ the general result that any local domain in K is dominated by a real discrete valuation ring in K, as proved in [1] or [4]. Furthermore, a closer look at the proof of this result in [4] shows that the residue field of the so obtained real discrete valuation ring has a dimension over the residue field $\bar{R}(\eta)$ of $\mathfrak{Q}(y(R)/\eta)$ which is exactly equal to the dimension of $\mathfrak{Q}(y(R)/\eta)$. The last condition in our lemma will then be fulfilled if we have the "dimension formula": $\dim(\mathfrak{Q}(y(R)/\eta)) + \dim(\eta/\bar{R}) = t$. This "dimension formula," in fact in a somewhat more general form, has been proved recently by Nagata [10] under the assumption that R satisfies the "second chain condition," and a previous result of Nagata shows that a unmixed local domain always satisfies this "second chain condition."

As a corollary to Lemma 2.7, we have the following useful lemma.

LEMMA 2.8. *If R is an analytically irreducible local domain, then $\bar{y}(R) = \bar{y}(R^*)$ for every rational transform $y(R)$ of R.*

Proof. Since R^* dominates R, it is clear that $\bar{y}(R^*) \subset \bar{y}(R)$; we have therefore only to show that every point in $\bar{y}(R)$ is also a point in $\bar{y}(R^*)$. Let η be a point in $\bar{y}(R)$ and let M be a real discrete valuation ring in K which dominates $Q(y(R)/\eta)$ and whose residue field has the dimension $t-1$ over $\bar{R}$ (t being the dimension of R). According to [13], Theorem 2, R is a subspace in M, so that the completion R^* of R can be embedded in the completion M^* of M; it is clear that M^* dominates both R^* and M. It follows that $\bar{y}(M^*)$ is a point in $\bar{y}(R^*)$ and also that $\bar{y}(M^*) = \bar{y}(M) = \eta$; this shows that η is a point in $y(R^*)$.

Before proceeding further, we shall make an observation here which will be useful to us also later. Let $v = (v_1, \cdots, v_d)$ be a set of independent variables over R, and consider the quotient ring $R(v)$ of $R[v]$ with respect to the prime ideal $R[v]\mathfrak{p}$; it is easily seen that $R(v)$ is a local domain of dimension t, with the quotient field $K(v)$, and that $R(v)$ is normal or regular if and only if R is such. Furthermore, if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in R, then we have $R(v)(\mathfrak{a} \cap \mathfrak{b}) = R(v)\mathfrak{a} \cap R(v)\mathfrak{b}$ and $R(v)\mathfrak{a} \cap R = \mathfrak{a}$, and if $\mathfrak{q}$ is a primary ideal in R with the associated prime ideal $\mathfrak{q}'$, then $R(v)$ is primary with

$R(v)\mathfrak{q}'$ as its associated prime. Finally, the $R(v)\mathfrak{p}$-residues $\bar{v} = (\bar{v}_1, \cdots, \bar{v}_d)$ of v are algebraically independent over $\bar{R}$, so that we can attach $R(v)$ to Λ by identifying the $\bar{v}$ with any set of d independent variables over $\bar{R}$; therefore, $R(v)$ dominates R and its residue field $\bar{R}(\bar{v})$ is a purely transcendental extension of dimension d over $\bar{R}$. For proof, we refer to [6], Lemma 14 for a part of it, with the remark that the rest of our assertions follows easily from it. In many problems these properties will enable us to replace the original local domain R by $R(v)$, and such a substitution often turns out to be convenient, mainly on account of the fact that the residue field $\bar{R}$ is thereby extended by the adjunction of an arbitrary number of variables and in particular made infinite. We shall call $R(v)$ the local domain obtained from R by the *adjunction of the variables* v.

Assume now that R is a complete regular local domain of dimension $t > 2$, and let $x_1, \cdots, x_t$ be the elements in a minimal base for $\mathfrak{p}$; then $R(v)$ is a regular local domain of dimension t and the elements $x_1, \cdots, x_t$ form also a minimal base for its maximal prime ideal $R(v)\mathfrak{p}$. Let $d \leqq t - 2$, and set $u_i = (x_2 + v_i x_{i+2})/x_1$ for $i = 1, \cdots, d$; denote by R_v the quotient ring of $R(v)[u_1, \cdots, u_d]$ with respect to the prime ideal $R(v)[u_1, \cdots u_d]\mathfrak{p}$. It is easily seen that R_v is a regular local domain of dimension $t - d$, and that the $R_v\mathfrak{p}$-residues $\bar{u} = (\bar{u}_1, \cdots, \bar{u}_d)$ of $u = (u_1, \cdots, u_d)$ are algebraically independent over $\bar{R}(\bar{v})$, so that we can attach R_v to by identifying $\bar{u}$ with any set of d independent variables over $\bar{R}(\bar{v})$. The following lemma, which can be considered as the local equivalent of the well-known "Theorem of Bertini" in algebraic geometry, plays an essential role later in the proof of Theorem 2 in that it enables us to reduce that theorem to the case $t = 2$.

LEMMA 2.9. *The quotient field K of R is algebraically closed in the quotient field of the completion R_v^* of R_v.*

This lemma is equivalent to the assertion that if a monic polynomial of one variable with coefficients in R is irreducible over R, then it is also irreducible over the completion R_v^* of R_v. We can evidently without any loss of generality restrict ourselves to the case $d = 1$, the general case following then by induction, and for this case the assertion can be proved in exactly the same way as the lemma in [5], except that one replaces the element c there by the element $v = v_1$ and observes that v satisfies the condition of being "sufficiently general" as required there. We therefore refer the proof of this lemma to [5].

3. Quadratic transforms and linear connectedness theorem. Let

$(R, \mathfrak{p})$ be a local domain of dimension t, with the quotient field K and the residue field $\bar{R}$, and let $x_1, \cdots, x_s$ be elements which form a minimal basis for $\mathfrak{p}$; if we denote by x the point $(x_1, \cdots, x_s)$ in S^{s-1}, then the rational transform $x(R)$ of R is called the *quadratic transform* of R. Since any two minimal bases for $\mathfrak{p}$ have the same number of elements and can be obtained each from the other by a linear transformation with coefficients in R and with determinant not in $\mathfrak{p}$, the quadratic transform $x(R)$ of R is unique up to an everywhere biregular transformation. We shall be mainly interested in the case where the local domain R is regular, and we recall that in this case the number s is equal to the dimension t. In this case, it is well-known ([1], Lemma 3, and Corollary 1) that $\bar{x}(R) = \bar{S}^{t-1}$ and every point in $\bar{x}(R)$ is simple in $x(R)$; furthermore ([2], Lemma 10, or as a special case of the dimension formula in [10]), if ξ is any point in $\bar{x}(R)$ and if t' is the dimension of $\mathfrak{Q}(x(R)/\xi)$, then $t' + \dim(\xi/\bar{R}) = t$. In case ξ is a generic point of $\bar{x}(R) = \bar{S}^{t-1}$ over $\bar{R}$, then $\mathfrak{Q}(x(R)/\xi)$ is a real discrete valuation ring, which (considered without its attachment to Λ) is the valuation ring of what is sometimes called the *$\mathfrak{p}$-adic valuation of R*; we shall call this valuation ring the *quadratic valuation ring* of R.

Let $y(R)$ be a rational transform of R in S^m, and let η be a point in $\bar{y}(R)$; let $\mathfrak{P}(\eta)$ be the homogeneous ideal in $R[Y] = R[Y_0, Y_1, \cdots, Y_m]$ generated by all forms $f(Y)$ such that $\bar{f}(\eta) = 0$, and let h be a positive integer such that there exists a basis of this ideal $\mathfrak{P}(\eta)$ consisting of forms of degrees less than $h+1$. Let $b_1(Y), \cdots, b_l(Y)$ be a basis of the R-module of all forms of degree h in $\mathfrak{P}(\eta)$, and denote the point $(b_1(y), \cdots, b_l(y))$ by b; if we set $z = y \circ b$, then the rational transform $z(R)$ is called the *quadratic transform of $y(R)$ centered at η*. This definition is analogous to the one given in [11], II, § 11 (for a monoidal transformation), and by a similar argument as given there, we can show that the quadratic transform $z(R)$ is up to an everywhere biregular birational correspondence independent of the choice of the integer h and the basis $b_1(Y), \cdots, b_l(Y)$, being dependent only on the point η. Furthermore, it is clear that $z(R)$ remains unchanged if we replace the point η by any one of its generic specializations over $\bar{R}$; this shows that the concept of a quadratic transform belongs really to the relative geometry.

Let T be the birational correspondence between $y(R)$ and its quadratic transform $z(R)$ centered at η. It is clear from the definition $z = y \circ b$ that the inverse T^{-1} is everywhere regular in $\bar{z}(R)$, and that T itself is regular at every point in $\bar{y}(R)$ which is not a specialization of η over $\bar{R}$. As to the point η itself, we can take any valuation ring M in K dominating $\mathfrak{Q}(y(R)/\eta)$

and get a point $\bar{z}(M) = \eta \circ \bar{b}(M)$ in $T(\eta)$, and in this way we can obtain every point in $T(\eta)$; it follows that $T(\eta) = \bar{z}(\mathfrak{Q}(y(R)/\eta)) = \eta \circ \bar{b}(\mathfrak{Q}(y(R)/\eta))$. Let $w_1, \cdots, w_\tau$ be the elements of a minimal basis for the maximal prime ideal in $\mathfrak{Q}(y(R)/\eta)$, and denote by w the point $(w_1, \cdots, w_\tau)$ in $S^{\tau-1}$. It is easily seen that the coordinates of b, after division by the form y_i^h if $\eta_i \neq 0$, are linear combinations of the coordinates of w with coefficients in $\mathfrak{Q}(y(R)/\eta)$, and vice-versa; therefore, the coordinates of z, after division by the form y_i^h, are also linear combinations of the coordinates of $y \circ w$ with coefficients in $\mathfrak{Q}(y(R)/\eta)$, and vice-versa. Since both

$$\mathfrak{Q}(z(R)/\bar{z}(M) \text{ and } \mathfrak{Q}(y \circ w(R)/\eta \circ \bar{w}(M))$$

contain $\mathfrak{Q}(y(R)/\eta)$ as a subring, it follows easily from this that

$$\mathfrak{Q}(z(R)/\bar{z}(M)) = \mathfrak{Q}(y \circ w(R)/\eta \circ \bar{w}(M));$$

furthermore, going over to the residue field of M, we conclude that the coordinates of $\bar{z}(M) = \eta \circ \bar{b}(M)$ and the coordinates of $\overline{y \circ w}(M) = \eta \circ \bar{w}(M)$ are linear combinations of each other with coefficients in $\bar{R}(\eta)$. This shows that the birational correspondence between $z(R)$ and $y \circ w(R)$ *is* biregular between $\bar{z}(\mathfrak{Q}(y(R)/\eta))$ and $\overline{y \circ w}(\mathfrak{Q}(y(R)/\eta))$, and that each $\bar{R}(\eta)$-variety in $T(\eta)$ is biregularly, in fact projectively equivalent over $\bar{R}(\eta)$ to an $\bar{R}(\eta)$-variety in $\eta \circ \bar{w}(\mathfrak{Q}(y(R)/\eta))$.

LEMMA 3.1. *For any valuation ring M in K dominating $\mathfrak{Q}(y(R)/\eta)$, we have the relation $\mathfrak{Q}(z(R)/\bar{z}(M)) = \mathfrak{Q}(w(\mathfrak{Q}(y(R)/\eta))/\bar{w}(M))$.*

Proof. Every element in $\mathfrak{Q}(w(\mathfrak{Q}(y(R)/\eta))/\bar{w}(M))$ is the quotient $f(w)/g(w)$ of two forms of the same degree in w with coefficients in $\mathfrak{Q}(y(R)/\eta)$, with the condition $\bar{g}(\bar{w}(M)) \neq 0$, while every element in $\mathfrak{Q}(y(R)/\eta)$ is the quotient $f'(y)/g'(y)$ of two forms of the same degree in y with coefficients in R, with the condition $\bar{g}'(\eta) \neq 0$; it follows that, by multiplying both $f(w)$ and $g(w)$ with a suitable power of a coordinate y_i or w_j such that the i-th coordinate of η or the j-th coordinate of $\bar{w}(M)$ does not vanish respectively, we can express any element in $\mathfrak{Q}(w(\mathfrak{Q}(y(R)/\eta))\bar{w}(M))$ as a quotient $f''(y \circ w)/g''(y \circ w)$ of two forms of the same degree in $y \circ w$ with coefficients in R, with the condition $g''(\eta \circ \bar{w}(M)) \neq 0$. This shows that

$$\mathfrak{Q}(w(\mathfrak{Q}(y(R)/\eta))/\bar{w}(M))$$

is contained in $\mathfrak{Q}(y \circ w(R)/\eta \circ \bar{w}(M)) = \mathfrak{Q}(z(R)/\bar{z}(M))$. In a similar way we can show that conversely $\mathfrak{Q}(z(R)/\bar{z}(M))$ is also contained in

$$\mathfrak{Q}(w(\mathfrak{Q}(y(R)/\eta))/\bar{w}(M)).$$

If the point η is simple in $y(R)$, then the local ring $\mathfrak{Q}(y(R)/\eta)$ is regular; it follows then from what we have said before about the quadratic transform of a regular local ring that (a) $\bar{w}(\mathfrak{Q}(y(R)/\eta)) = \bar{S}^{\tau-1}$, (b) $w(\mathfrak{Q}(y(R)/\eta))$ is simple at every point $\bar{w}(M)$ in $\bar{w}(\mathfrak{Q}(y(R)/\eta))$, and (c) if τ' is the dimension of the local ring $\mathfrak{Q}(w(\mathfrak{Q}(y(R)/\eta))/\bar{w}(M))$, then $\tau' + \dim(\bar{w}(M)/\bar{R}(\eta)) = \tau$. In view of Lemma 3.1 and the remarks immediately preceding it, we can conclude in this case that (a) $T(\eta)$ consists of a single $(\tau-1)$-dimensional variety, defined over $\bar{R}(\eta)$, and there is a biregular birational transformation Ψ, defined over $\bar{R}(\eta)$, which maps $\bar{w}(\mathfrak{Q}(y(R)/\eta)) = \bar{S}^{\tau-1}$ onto $T(\eta)$; (b) $z(R)$ is simple at every point $\bar{z}(M)$ in $T(\eta)$; and (c) τ' is also the dimension of the local ring $\mathfrak{Q}(z(R)/\bar{z}(M))$ and we have the relation $\tau' + \dim(\bar{z}(M)/\bar{R}(\eta)) = \tau$.

We shall now assume further that the point η (already assumed to be simple in $y(R)$) is contained in a variety Ω in $\bar{y}(R)$ with the following properties: (1) Ω is defined over an extension field Δ of $\bar{R}$ such that if $\sigma-1$ is the dimension of Ω, then we have the equation $\sigma + \dim(\Delta/\bar{R}) = t$; (2) if ξ is any point in Ω, then $\bar{R}(\xi)$ contains Δ; (3) every point in Ω is simple in $y(R)$; (4) there is a biregular transformation Φ, defined over Δ, which maps the projective space $\bar{S}^{\sigma-1}$ onto Ω. Let ζ be a generic point of Ω over Δ, and let ζ' be a generic point of $T(\eta)$ over $\bar{R}(\eta)$; we shall prove the following lemma, which plays an essential part in the proof of Theorem 1 later.

LEMMA 3.2. *There exists a linearly connected set Γ in $\bar{z}(R)$ with the properties:* (1) *Γ contains both $T(\zeta)$ and ζ', and* (2) *every point in Γ is simple in $z(R)$ and has a dimension at least $t-2$ over $\bar{R}$, and* (3) *Γ consists of a finite number of rational curves.*

Proof. Since the point η is a specialization of the point ζ over $\bar{R}$, in fact over Δ, the local ring $\mathfrak{Q}(y(R)/\zeta)$ is the quotient ring of the local ring $\mathfrak{Q}(y(R)/\eta)$ with respect to a prime ideal $\mathfrak{p}_0$, which must then necessarily be of rank 1 (for $\mathfrak{Q}(y(R)/\zeta)$ has the dimension 1). The residue ring $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$ is then canonically isomorphic to a subring in the residue field $\bar{R}(\zeta) = \Delta(\zeta)$ of $\mathfrak{Q}(y(R)/\zeta)$; in fact, it is easily seen that this subring is precisely the specialization ring $\mathfrak{Q}(\zeta/\eta, \Delta)$ in $\Delta(\zeta)$ of the variety Ω at the point η. For the sake of convenience, we shall identify the residue ring $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$ with $\mathfrak{Q}(\zeta/\eta, \Delta)$; this implies in particular that we shall identify the residue field of the local ring $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$ with $\bar{R}(\eta) = \Delta(\eta)$, and in this way attach $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$ to Λ. Since Ω is biregularly equivalent over Δ to the projective space $\bar{S}^{\sigma-1}$, and since it is well-known (see [11], Lemma 9, p. 541) that the specialization ring over Δ of $\bar{S}^{\sigma-1}$ at any point is a

regular local ring whose dimension is equal to $\sigma - 1$ minus the dimension of the point over Δ, it follows that $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$ is a regular local ring of dimension $\sigma - 1 - \dim(\eta/\Delta)$. Since $\mathfrak{Q}(y(R)/\eta)$ is itself a regular local ring, it follows from a well-known result ([3], § III, Proposition 9, p. 705) that the basis $w_1, \cdots, w_\tau$ of $\mathfrak{Q}(y(R)/\eta)$ can be so chosen that $\mathfrak{p}_0$ is the principal ideal (w_τ) generated by the one element w_τ, and that the canonical images $\omega_1, \cdots, \omega_{\tau-1}$ of $w_1, \cdots, w_{\tau-1}$ in $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$ coincide with any given minimal basis for its maximal prime ideals; furthermore, we have evidently the relation $\dim(\eta/\Delta) = \sigma - \tau$, and since $\bar{R}(\eta)$ contains Δ, it follows that $\dim(\eta/\bar{R}) = \dim(\eta/\Delta) + \dim(\Delta/\bar{R}) = t - \tau$. Now, let M be the quadratic valuation ring of the regular local ring $\mathfrak{Q}(y(R)/\eta)/\mathfrak{p}_0$; we shall attach M to Λ in such a way that its residue field M contains $\bar{R}(\eta)$ and is free with respect to $\bar{R}(\zeta')$ over $\bar{R}(\eta)$. If we denote by ω the point in $S^{\tau-1}$ (observe that by our convention $\bar{S}^{\tau-1}$ is contained in $S^{\tau-1}$) with the projective coordinates $(\omega_1, \cdots, \omega_{\tau-1}, 0)$, then the point $\bar{\omega}(\mathrm{M})$ in $\bar{S}^{\tau-1}$ has the form $(\lambda_1, \cdots, \lambda_{\tau-1}, 0)$, where $\lambda_1 = 1$, and $\lambda_2, \cdots, \lambda_{\tau-1}$ are independent variable (in Λ) over $\Delta(\eta)$. Let M be the valuation ring of the composite valuation obtained from the valuation of $\mathfrak{Q}(y(R)/\zeta)$ and the valuation of its residue field determined by M, i. e. the ring M consists of all elements in $\mathfrak{Q}(y(R)/\zeta)$ whose images in the residue field are contained in the ring M; we shall attach M to Λ by identifying its residue field with the residue field of M. It is clear that M dominates $\mathfrak{Q}(y(R)/\eta)$, so that $\bar{z}(M)$ is a point in $T(\eta)$. Furthermore, it follows from the definition of a composite valuation that $\bar{w}(M) = \bar{\omega}(\mathrm{M}) = (\lambda_1, \cdots, \lambda_{\tau-1}, 0)$; since $\bar{R}(\eta, \bar{z}(M)) = \bar{R}(\eta, \bar{w}(M))$, the point $\bar{z}(M)$ has the dimension $\tau - 2$ over $\bar{R}(\eta)$, and since $\bar{R}(\bar{z}(M))$ contains $\bar{R}(\eta)$, by the relation $\eta = T^{-1}(\bar{z}(M))$, the point $\bar{z}(M)$ has the dimension $\tau - 2 + \dim(\eta/\bar{R}) = t - 2$ over $\bar{R}$. If we denote by Γ' the line in $\bar{S}^{\tau-1}$ joining the points $\bar{w}(M)$ and $\Psi^{-1}(\zeta')$, then it is easily seen that every point in Γ' has a dimension at least $\tau - 2$ over $\bar{R}(\eta)$; going over to the variety $T(\eta)$, we obtain a rational curve $\Psi(\Gamma')$ in $T(\eta)$ which contains both $\bar{z}(M)$ and ζ', such that every point on it has a dimension at least $\tau - 2$ over $\bar{R}(\eta)$. Since every point in $\Psi(\Gamma')$ has the point η as its image under the holomorphic rational mapping T^{-1} (of $z(R)$) and since $\dim(\eta/\bar{R}) = t - \tau$, it follows that every point in $\Psi(\Gamma')$ has a dimension at least $t - 2$ over $\bar{R}$; furthermore, every point in $\Psi(\Gamma')$, being a point in $T(\eta)$, is simple in $z(R)$. This shows that the curve $\Gamma_1 = \Psi(\Gamma')$ has the property (2) in our lemma.

We set $\theta = (\theta_1, \cdots, \theta_\sigma) = \Phi^{-1}(\zeta)$ and $\alpha = (\alpha_1, \cdots, \alpha_\sigma) = \Phi^{-1}(\eta)$; we observe that $\mathfrak{Q}(\zeta/\eta, \Delta)$ is also the specialization ring $\mathfrak{Q}(\theta/\alpha, \Delta)$ in $\Delta(\theta) = \Delta(\zeta)$ of $\bar{S}^{\sigma-1}$ at the point α, so that the elements $\omega_1, \cdots, \omega_{\tau-1}$ form also a basis for

the maximal prime ideal in $\mathfrak{Q}(\theta/\alpha,\Delta)$. We shall show below that there exists a rational curve Γ'' in $\bar{S}^{\sigma-1}$ containing the points θ and α, with the property that every point in Γ'' except possibly α has a dimension at least $\sigma-2$ over Δ and that the elements ω_i/ω_1, $i=2,\cdots,\tau-1$, considered as function on Γ'', have values at α which are independent variables over $\Delta(\alpha)$. Going over to the variety Ω, we have a rational curve $\Phi(\Gamma'')$ containing the points ζ and η such that every point in $\Phi(\Gamma'')$ except possibly η has a dimension at least $\sigma-2$ over Δ and hence a dimension at least $t-2$ over $\bar{R}$. Since the values of ω_i/ω_1, $i=2,\cdots,\tau-1$, on $\Phi(\Gamma'')$ at the point η are independent variables over $\Delta(\alpha)=\bar{R}(\eta)$, we can take them to be the elements $\lambda_2,\cdots,\lambda_{\tau-1}$ introduced before; then in the "proper transform" of $\Phi(\Gamma'')$ in $\overline{y\circ\bar{w}}(R)$, i.e. the locus over the defining field of $\Phi(\Gamma'')$ of the image in $\overline{y\circ\bar{w}}(R)$ of a generic point of $\Phi(\Gamma'')$, the (unque) point corresponding to η is $\eta\circ\bar{w}(M)$. Let Γ_2 be the "proper transform" of $\Phi(\Gamma'')$ in $\bar{z}(R)$; it is clear that Γ_2 contains the point $T(\zeta)$. Since the correspondence T is biregular at every point in $\Phi(\Gamma'')$ except η, it follows that every point in Γ_2 outside of $T(\eta)$ has a dimension at least $t-2$ over $\bar{R}$; on the other hand, since the correspondence between $z(R)$ and $y\circ w(R)$ is biregular at every point in $T(\eta)$, it follows that $\bar{z}(M)$ is the (unique) point on Γ_2 corresponding to η in $\Phi(\Gamma'')$. This shows that Γ_2 contains the points $\bar{z}(M)$ and $T(\zeta)$, and has the property (2) in our lemma. If we set $\Gamma=\Gamma_1+\Gamma_2$, then Γ is clearly linearly connected and has the properties (1), (2) and (3) in our lemma.

It remains therefore to prove the existence of the curve Γ''. For convenience we shall assume that ζ is a generic point of Ω over $\bar{R}(\eta)$, not only over Δ; this does not essentially affect our situation, for if Γ_2 does not contain ζ, but contains another generic point χ of Ω over Δ, then we can take a line Γ''' in $\bar{S}^{\sigma-1}$ joining θ and $\Phi^{-1}(\chi)$ and replace Γ by $\Gamma+T(\Phi(\Gamma'''))$. Also, without any loss of generality, we can assume that $\theta_\sigma=\alpha_\sigma=1$ and that $\alpha_\tau,\cdots,\alpha_{\sigma-1}$ are independent variables over Δ; we observe that since θ is a generic point of $\bar{S}^{\sigma-1}$ over $\Delta(\alpha)$, the elements $\theta_1,\cdots,\theta_{\sigma-1}$ are independent variables over $\Delta(\alpha)$. Finally, we recall that we can choose the basis $\omega_1,\cdots,\omega_{\tau-1}$ in any way to suit our convenience; besides, the choice of this basis does not matter any way in our present context, for any two such bases can be obtained one from the other by a linear transformation with coefficients in $\mathfrak{Q}(\theta/\alpha,\Delta)$ and with determinant which is a unit.

For $i=1,\cdots,\tau-1$, let ω_i be an element in $\Delta[\theta_1,\cdots,\theta_i,\theta_\tau,\cdots,\theta_{\sigma-1}]$ which on substituting $\theta_1=\alpha_1,\cdots,\theta_{i-1}=\alpha_{i-1}$, $\theta_\tau=\alpha_\tau,\cdots,\theta_{\sigma-1}=\alpha_{\sigma-1}$ becomes an irreducible polynomial in $\Delta(\alpha_1,\cdots,\alpha_{i-1},\alpha_\tau,\cdots,\alpha_{\sigma-1})[\theta_i]$ having α_i as a root. It can be easily shown by induction on the dimension $\tau-1$ that

the elements $\omega_1, \cdots, \omega_{\tau-1}$ form a minimal basis for the maximal prime ideal in $\mathfrak{Q}(\theta/\alpha, \Delta)$, this being in fact the proof in [11], Lemma 9. If we denote by s_i the inseparability index of x_i over $\Delta(\alpha_1, \cdots, \alpha_{i-1}, \alpha_\tau, \cdots, \alpha_{\sigma-1})$, then we can evidently choose ω_i so that it involves only the s_i-th power of θ_i. Now, by a reordering of the first $\tau - 1$ coordinates in $\bar{S}^{\sigma-1}$ if necessary, we can evidently obtain that the sequence of integers $s_1, \cdots, s_{\tau-1}$ has the property that if $s'_1, \cdots, s'_{\tau-1}$ is another such sequence corresponding to any other ordering of the first $\tau - 1$ coordinates in $\bar{S}^{\sigma-1}$, then the last non-vanishing number in the sequence $s'_1 - s_1, \cdots, s'_{\tau-1} - s_{\tau-1}$ is positive. Then, for $j < i \leqq \tau - 1$, the inseparability index of α_j over $\Delta(\alpha_1, \cdots, \alpha_{j-1}, \alpha_{j+1}, \cdots, \alpha_i, \alpha_\tau, \cdots, \alpha_{\sigma-1})$ cannot be less than s_i; for, if this is not true for one such pair of indices i and j, and if we interchange the i-th and the j-th coordinates, then we would obtain a new sequence $s'_1, \cdots, s'_{\tau-1}$ such that $s_{i+1} = s'_{i+1}, \cdots, s_{\tau-1} = s'_{\tau-1}$, and $s'_i < s_i$, in contradiction to our choice of the sequence $s_1, \cdots, s_{\tau-1}$. Consider now ω_i as a polynomial in one variable θ_j $(j < i)$ with coefficients in $\Delta[\theta_1, \cdots, \theta_{j-1}, \theta_{j+1}, \cdots, \theta_i, \theta_\tau, \cdots, \theta_{\sigma-1}]$; it is clear that in our choice of ω_i we can delete any term whose coefficient vanishes for $\theta = \alpha$. If we delete all such terms from ω_i, then the resulting ω_i will involve only the s_i-th powers of θ_j; for, otherwise, if we set $\theta = \alpha$ in every coefficient in ω_i (considered as a polynomial in θ_j), we would obtain a polynomial in θ_j with coefficients in $\Delta(\alpha_1, \cdots, \alpha_{j-1}, \alpha_{j+1}, \cdots, \alpha_i, \alpha_\tau, \cdots, \alpha_{\sigma-1})$ which has α_j as a root and which is not a polynomial in the s_i-th power of θ_j, in contradiction to the fact that the inseparability index of α_j over $\Delta(\alpha_1, \cdots, \alpha_{j-1}, \alpha_{j+1}, \cdots, \alpha_\tau, \cdots, \alpha_{\sigma-1})$ cannot be less than s_i. If we do this for every $j < i$, we would then obtain that ω_i involves only the s_i-th powers of the elements $\theta_1, \cdots, \theta_i$. Thus we have shown that the elements $\omega_1, \cdots, \omega_{\tau-1}$ can be so chosen that each ω_i on substituting $\theta_\tau = \alpha_\tau, \cdots, \theta_{\sigma-1} = \alpha_{\sigma-1}$ becomes a polynomial in the s_i-th powers of $\theta_1, \cdots, \theta_i$; this implies that over an algebraic (purely inseparable) extension Δ' of $\Delta(\alpha)$, each ω_i will have the form $\omega_i = \phi_i(\theta_1 - \alpha_1, \cdots, \theta_i - \alpha_i)^{s_i} + \rho_i$, where ϕ_i is a ploynomial with coefficients in Δ' and ρ_i is an element in $\Delta'[\theta_1, \cdots, \theta_{\sigma-1}]$ which vanishes for $\theta_\tau = \alpha_\tau, \cdots, \theta_{\sigma-1} = \alpha_{\sigma-1}$. Furthermore, it is clear that $\phi_i(0, \cdots, 0) = 0$ and that the coefficient β_i of the term $(\theta_i - \alpha_i)^{s_i}$ in ϕ_i does not vanish; it follows that there exists a power series $\psi_i(\theta_1 - \alpha_1, \cdots, \theta_{i-1} - \alpha_{i-1})$ in $\theta_1 = \alpha_1, \cdots, \theta_{i-1} - \alpha_{i-1}$ with coefficients in Δ' such that $\phi_i(\theta_1 - \alpha_1, \cdots, \theta_{i-1} - \alpha_{i-1}, \psi_i) = 0$.

Let $\mu_1, \cdots, \mu_{\sigma-1}$ be independent variables over $\Delta'(\theta)$; for convenience in notation, we set $s_i = 1$ and $\psi_i = 0$ for $i = \tau, \cdots, \sigma - 1$. We define a curve Γ'' in $\bar{S}^{\sigma-1}$ by the following recursive parametric equations, where $Y_1, \cdots, Y_{\sigma-1}$

denote the (affine) coordinates in $\bar{S}^{\sigma-1}$ (with $Y_\sigma = 1$) and T denotes the parameter:

$$Y_i = \alpha_i + \mu_i T^{(s/s_i)} - \psi_i(Y_1 - \alpha_1, \cdots, Y_{i-1} - \alpha_{i-1})_s + \nu_i T^{s+1},$$

for $i = 1, \cdots, \sigma - 1$, where the $Y_1, \cdots, Y_{i-1}$ on the right hand side are to be substituted by their expressions in the previous equations, and the subscript s after the ψ_i indicates that all terms of degrees higher than s are to be deleted; furthermore, each ν_i is to be determined by the condition $\nu_i = \theta_i - \alpha_i - \mu_i + [\psi_i(Y_1 - \alpha_1, \cdots, Y_{i-1} - \alpha_{i-1})_s]_{T=1}$. It is easily seen that Γ'' is a rational curve and contains the points α (for $T = 0$) and θ (for $T = 1$). Furthermore, if $\Gamma''(\gamma)$ is the point on Γ'' corresponding to any value $\gamma \neq 0$ of T, then $\Delta'(\mu, \nu)$ is contained in $\Delta'(\gamma, \Gamma''(\gamma), \nu)$, and since $\Delta'(\mu, \nu)$ has the dimension $\sigma - 1$ over $\Delta'(\nu)$, it follows that $\Gamma''(\gamma)$ must have a dimension at least $\sigma - 2$ over $\Delta'(\nu)$. For $T = \infty$, the corresponding point on Γ'' has the homogeneous coordinates $(\nu_1, \cdots, \nu_{\sigma-1}, 0)$ and hence has the dimension $\sigma - 2$ over $\Delta'(\mu)$. Thus every point on Γ'', except possibly the point α, has a dimension at least $\sigma - 2$ over Δ. Finally, a simple calculation shows that each ω_i, considered as a function on Γ'', has at the point α a power series development in T beginning with the term $(\beta_i \mu_i + \delta_i) T^s$, where δ_i is an element in $\Delta'(\theta_1, \cdots, \theta_{i-1})$; this shows that the ratios ω_i/ω_1, $i = 2, \cdots, \tau - 1$, considered as functions on Γ'', have values at α which are independent variables over $\Delta(\alpha)$. This concludes the proof of Lemma 3.2.

Remark. If $\sigma = 2$, then Ω is a rational curve already and the rather complicated construction of the curve Γ'' is not necessary. In this case, the curve Ω can contain only a finite number of fundamental points $\eta^{(1)}, \cdots, \eta^{(d)}$ for T, and each set $T(\eta^{(i)})$ is also a rational curve with the property (2). It is clear that the set $T(\Omega)$ consists of the "proper transform" of Ω and all the curves $T(\eta^{(1)}), \cdots, T(\eta^{(d)})$, and that it is a connected set with the properties (2) and (3).

Let M be a valuation ring in K dominating R. We start with a rational transform $y(R)$ of R, and obtain from it a sequence of rational transforms $z^{(i)}(R)$ of R, $i = 1, 2, \cdots$, such that each $z^{(i)}(R)$ is the quadratic transform of $z^{(i-1)}(R)$ centered at $\bar{z}^{(i-1)}(M)$, whereby we set $z^{(0)}(R) = y(R)$. We shall say that $z^{(i)}(R)$ is the *i-th quadratic transform of* $y(R)$ *along* M. As we have observed above, if $y(M)$ is simple in $y(R)$, then $\bar{z}^{(i)}(M)$ will also be simple in $z^{(i)}(R)$ for every i; and, in this case, if we denote by t_i the dimension of $\mathfrak{Q}(z^{(i)}(R)/\bar{z}^{(i)}(M))$, then we have the relation $t_i + \dim(\bar{z}^{(i)}(M)/\bar{R}(\bar{z}^{(i-1)}(M))) = t_{i-1}$, for every $i = 1, 2, \cdots$, while for $i = 0$ we have the relation

$t_0 + \dim(\bar{z}^{(0)}(M)/\bar{R}) = t$. Since the birational correspondence between $z^{(i-1)}(R)$ and $z^{(i)}(R)$ is everywhere regular in $z^{(i)}(R)$, it follows that $\bar{R}(z^{(i)}(M))$ contains $\bar{R}(\bar{z}^{(i-1)}(M))$; we obtain therefore by addition the relation $t_i + \dim(\bar{z}^{(i)}(M)/\bar{R}) = t$ for every $i = 0, 1, \cdots$. We shall say that the sequence $z^{(i)}(R)$ of quadratic transforms of $y(R)$ along M is *finite* if there exists an index i such that $t_i = 1$ or equivalently $\dim(\bar{z}^{(i)}(M)/\bar{R}) = t - 1$. It is clear that this is possible only when the residue field of M has a dimension at least $t - 1$ over $\bar{R}$; according to [2], Theorem 1, this implies that M is a real discrete valuation ring and that its residue field has exactly the dimension $t - 1$ over $\bar{R}$. It is important for our present purpose that the converse of this statement is also true.

LEMMA 3.3. *If M is a real discrete valuation ring in $\mathfrak{V}(R)$ such that its residue field has the dimension $t-1$ over $\bar{R}$, and if $y(R)$ is a rational transform of R such that $y(M)$ is simple in $y(R)$, then the sequence of quadratic transforms of $y(R)$ along M is finite.*

A proof of this lemma is given in [2], Proposition 3.

We are now ready to prove the Linear Connectedness Theorem.

THEOREM 1 (Linear Connectedness Theorem). *The center $\bar{y}(R)$ of a rational transform $y(R)$ of a regular local ring R is linearly connected.*

Proof. As before, we denote by t, K, and $\bar{R}$ the dimension, the quotient field, and the residue field respectively of R. Consider the quadratic transform $z^{(1)}(R)$ of R and let T_1 be the birational correspondence between $z^{(1)}(R)$ and $y(R)$; if $\zeta^{(1)}$ is a generic point of $\bar{z}^{(1)}(R)$ over $\bar{R}$ (observe that $\bar{z}^{(1)}(R) = \bar{S}^{t-1}$), then T_1 is regular at $\zeta^{(1)}$ and hence $T_1(\zeta^{(1)})$ is a uniquely determined point in $\bar{y}(R)$, which we shall denote by ζ. To prove our theorem, it is sufficient to show that any point η in $\bar{y}(R)$ is linearly connected in $\bar{y}(R)$ to this point ζ. By Lemma 2.7, there exists a real discrete valuation ring M in $\mathfrak{V}(R)$, with a residue field which has the dimension $t-1$ over $\bar{R}$, such that $\bar{y}(M) = \eta$. For $1 < i \leqq a$ (the integer a will be determined presently), let $z^{(i)}(R)$ be the $(i-1)$-th quadratic transform of $z^{(1)}(R)$ along M, and let T_i be the birational correspondence between $z^{(i)}(R)$ and $y(R)$. We set $T_{i,j} = T_j^{-1}T_i$ for $i, j = 1, \cdots, a$, so that $T_{i,j}$ is the birational correspondence between $z^{(i)}(R)$ and $z^{(j)}(R)$; we set $\eta^{(i)} = \bar{z}^{(i)}(M)$ for $i = 1, \cdots, a$, and take for each $i = 2, \cdots, a$, a generic point $\zeta^{(i)}$ of the variety $T_{i-1,i}(\eta^{(i-1)})$ over $\bar{R}(\eta^{(i-1)})$. The integer a is to be taken as the smallest integer such that the point $\eta^{(a)} = \bar{z}^{(a)}(M)$ has the dimension $t-1$ over $\bar{R}$; by Lemma 3.3, such an integer a exists, and since $\eta^{(a)}$ is simple in $z^{(a)}(R)$, it must be a regular

point of T_a and we have evidently $\eta = T_a(\eta^{(a)})$. Furthermore, since $\eta^{(a)}$ has the dimension $t-1$ over $\bar{R}$, it must have the maximum possible dimension over $\bar{R}(\eta^{(a-1)})$ and hence is a generic point of $T_{a-1,a}(\eta^{(a-1)})$ over $\bar{R}(\eta^{(a-1)})$; we can therefore take $\eta^{(a)}$ itself as the point $\zeta^{(a)}$, which will be convenient for us later. We maintain now that there exists a connected set $\Gamma^{(i)}$ in $\bar{z}^{(i)}(R)$ with the following properties: (1) $\Gamma^{(i)}$ contains both $\zeta^{(i)}$ and $T_{1,i}(\zeta^{(1)})$, (2) every point in $\Gamma^{(i)}$ is simple in $z^{(i)}(R)$ and has a dimension at least $t-2$ over $\bar{R}$, and (3) $\Gamma^{(i)}$ consists of either a single point or a finite number of rational curves. We shall show this by induction on the index i, beginning by setting $\Gamma^{(1)} = \zeta^{(1)}$, and, assuming the induction hypothesis that the set $\Gamma^{(i-1)}$ has already been constructed, we shall proceed to contruct the set $\Gamma^{(i)}$. If $T_{i-1,i}$ has no fundamental points in $\Gamma^{(i-1)}$ and hence is biregular everywhere in $\Gamma^{(i-1)}$, then the set $T_{i-1,i}(\Gamma^{(i-1)})$ is evidently connected, has the properties (2) and (3), and contains the points $T_{1,i}(\zeta^{(1)}) = T_{i-1,i}(T_{1,i-1}(\zeta^{(1)}))$ and $T_{i-1,i}(\zeta^{(i-1)})$. Assuming now that $T_{i-1,i}$ has some fundamental points in $\Gamma^{(i-1)}$; we observe that this can occur only if $\dim(\eta^{(i-1)}/\bar{R}) = t-2$, in which case $T_{i-1,i}$ can have only a finite number of fundamental points $\eta^{(i-1,1)}, \cdots, \eta^{(i-1,b)}$ in $\Gamma^{(i-1)}$, all of dimension $t-2$ over $\bar{R}^{-(i-1)}$, and each set $T_{i-1,i}(\eta^{(i-1,j)})$ is a rational curve in $\bar{z}^{(i)}(R)$ which has the property (2). If we denote by $\Gamma_1^{(i-1)}, \cdots, \Gamma_c^{(i-1)}$ the distinct component curves in $\Gamma^{(i-1)}$, then by the Remark after Lemma 3.2 each set $T_{i-1,i}(\Gamma_k^{(i-1)})$ is connected and has the properties (2) and (3), and it will contain the curve $T_{i-1,i}(\eta^{(i-1,j)})$ whenever $\Gamma_k^{(i-1)}$ contains the point $\eta^{(i-1,j)}$. It follows then from an elementary combinatorial consideration that the set $T_{i-1,i}(\Gamma^{(i-1)}) = \sum_{k=1}^{c} T_{i-1,i}(\Gamma_k^{(i-1)})$ is connected, and it evidently has the properties (2) and (3), and contains the point $T_{1,i}(\zeta^{(1)})$ and $T_{i-1,i}(\zeta^{(i-1)})$. Now, by Lemma 3.2, there exists a connected set Γ_i in $\bar{z}^{(i)}(R)$ which has the properties (2) and (3) and contains the points $\zeta^{(i)}$ and $T_{i-1,i}(\zeta^{(i-1)})$. The set $\Gamma^{(i)} = T_{i-1,i}(\Gamma^{(i-1)}) + \Gamma_i$ is then evidently connected and has the properties (1), (2), and (3).

For $i = a$, we obtain a linearly connected set $\Gamma^{(a)}$ in $\bar{z}^{(a)}(R)$ which has the properties (2) and (3) and which contains the points $T_{1,a}(\zeta^{(1)})$ and $\bar{z}^{(a)}(M) = \eta^{(a)} = \zeta^{(a)}$. If T_a is regular at every point in $\Gamma^{(a)}$, then T_a induces a continuous mapping of $\Gamma^{(a)}$ into $\bar{y}(R)$, so that $T_a(\Gamma^{(a)})$ is a linearly connected set; since $T_a(\Gamma^{(a)})$ contains the points $\zeta = T_1(\zeta^{(1)}) = T_a(T_{1,a}(\zeta^{(1)}))$ and $\eta = T_a(\eta^{(a)}) = T_a(\zeta^{(a)})$, our theorem would therefore be proved. Otherwise, we proceed as follows. Consider the join $y \circ z^{(a)}(R)$, and let T_a' be the birational correspondence between $z^{(a)}$ and $y \circ z^{(a)}(R)$. By Lemma 2.5, there exist in $\overline{y \circ z}^{(a)}(R)$ only a finite number of points of dimension $t-1$ over $\bar{R}$

such that no two of them are equivalent over $\bar{R}$ (i.e. specializations of each other over $\bar{R}$), and by Lemma 2.6, there exist only a finite number of valuation rings in $\mathfrak{V}(R)$ whose centers in $y \circ z^{(a)}(R)$ coincide with any one of these points, and these valuation rings are all real discrete. There exist therefore a finite number of real discrete valuation rings $M_1, \cdots, M_d$ in $\mathfrak{V}(R)$ such that any valuation ring in $\mathfrak{V}(R)$ whose center in $y \circ z^{(a)}(R)$ has the dimension $t-1$ over $\bar{R}$ coincides with one of them up to attachments to Λ. If T_a is not regular at a point ξ in $\Gamma^{(a)}$, then T_a' also cannot be regular at ξ; since ξ is simple and hence normal in $z^{(a)}(R)$, it follows from Lemma 2.4 that $T_a'(\xi)$ has at least one component of positive dimension. There exists therefore a valuation ring N in $\mathfrak{V}(R)$ such that $\bar{z}^{(a)}(N) = \xi$ and such that the point $\overline{y \circ z}^{(a)}(N)$ has a positive dimension over $\bar{R}(\xi)$. Since $T_a'^{-1}$ is regular everywhere, $\bar{R}(\overline{y \circ z}^{(a)}(N))$ must contain $\bar{R}(\xi)$ as subfield, and since ξ has the dimension $t-2$ over $\bar{R}$, it follows that $\overline{y \circ z}^{(a)}(N)$ has the dimension $t-1$ over $\bar{R}$. From what we have just said, N must coincide up to attachment to Λ with one of the valuation rings M_i, say M_1, so that $z^{(a)}(M_1)$ is equivalent to ξ over $\bar{R}$ and hence is also simple in $z^{(a)}(R)$. Now, let $z^{(i)}(R)$, for $a < i \leqq a_1$ (the integer a_1 will be determined presently), be the $(i-a)$-th quadratic transform of $z^{(a)}(R)$ along M_1, and let T_i be as before the birational correspondence between $z^{(i)}(R)$ and $y(R)$; also as before, we set $T_{i,j} = T_j^{-1}T_i$, so that $T_{i,j}$ is the birational correspondence between $z^{(i)}(R)$ and $z^{(j)}(R)$. If we set $\Gamma^{(i)} = T_{i-1,i}(\Gamma^{(i-1)}) = T_{a,i}(\Gamma^{(a)})$, then by exactly the same induction argument as before we can show that $\Gamma^{(i)}$ is a linearly connected set with the properties (2) and (3), and it is evident that $\Gamma^{(i)}$ contains the points $T_{1,i}(\zeta^{(1)}) = T_{a,i}(T_{1,a}(\zeta^{(1)}))$ and $\bar{z}^{(i)}(M) = T_{a,i}(\eta^{(a)})$. By Lemma 3.3, there exists a smallest integer $a_1 > a$ such that the point $\bar{z}^{(a_1)}(M_1)$ has the dimension $t-1$ over $\bar{R}$, so that T_{a_1} is regular at $\bar{z}^{(a_1)}(M_1)$; this determines a_1. If T_{a_1} is regular at every point in $\Gamma^{(a_1)}$, then T_{a_1} induces a continuous mapping of $\Gamma^{(a_1)}$ into $\bar{y}(R)$ and hence $T_{a_1}(\Gamma^{(a_1)})$ is a linearly connected set; since $T_{a_1}(\Gamma^{(a_1)})$ contains the points $\zeta = T_1(\zeta^{(1)}) = T_{a_1}(T_{1,a_1}(\zeta^{(1)}))$ and $\eta = T_{a_1}(\bar{z}^{(a_1)}(M))$, this would prove our theorem. If T_{a_1} is not regular at some one point $\xi^{(1)}$ in $\Gamma^{(a_1)}$, then by the same argument as before we can show that there exists a valuation ring N_1 in $\mathfrak{V}(R)$ such that $\bar{z}^{(a_1)}(N_1) = \xi^{(1)}$ and such that the point $\overline{y \circ z}^{(a_1)}(N_1)$ has the dimension $t-1$ over $\bar{R}$. Since $\bar{z}^{(a)}(N_1)$ is a point in $\Gamma^{(a)}$, it must have the same dimension $t-2$ over $\bar{R}$ as the point $\bar{z}^{(a_1)}(N_1)$; it follows that the point $\bar{z}^{(a_1)}(N_1)$ is algebraic over $\bar{R}(\bar{z}^{(a)}(N_1))$, and hence the point $\overline{y \circ z}^{(a_1)}(N_1)$ must be algebraic over $\bar{R}(\overline{y \circ z}^{(a)}(N_1))$. This shows that the point $\overline{y \circ z}^{(a)}(N_1)$ has the dimension $t-1$ over $\bar{R}$, and it follows from what we have said before that N_1 must coincide up to attachments to Λ with one

of the valuation rings M_i, say M_2. We can then proceed in a similar way with $z^{(a)}(R)$, $\Gamma^{(a_1)}$, M_2 as we did before with $z^{(a)}(R)$, $\Gamma^{(a)}$ M_1. Thus we proceed in this way step by step until, after a finite number π of steps, we have obtained a rational transform $z^{(\pi)}(R)$ of R with the following properties, whereby T_π and $T_{1,\pi}$ have similar meanings as before: There exists a linearly connected set $\Gamma^{(\pi)}$ in $\bar{z}^{(\pi)}(R)$ which has the properties (2) and (3) and which contains the points $T_{1,\pi}(\zeta^{(1)})$ and $\bar{z}^{(\pi)}(M)$, and for every M_i the point $\bar{z}^{(\pi)}(M_i)$ either has the dimension $t-1$ over $\bar{R}$ or is not equivalent over $\bar{R}$ to a point in $\Gamma^{(\pi)}$. From what we have said above, this implies that T_π is regular at every point in $\Gamma^{(\pi)}$. Therefore T_π induces a continuous mapping of $\Gamma^{(\pi)}$ into $\bar{y}(R)$, so that $T_\pi(\Gamma^{(\pi)})$ is a linearly connected set; since $T_\pi(\Gamma^{(\pi)})$ contains the points $\zeta = T_1(\zeta^{(1)}) = T_\pi(T_{1,\pi}(\zeta^{(1)}))$ and $\eta = T_\pi(\bar{z}^{(\pi)}(M))$, this concludes the proof of Theorem 1.

Corollary 1. *In case $t = 2$, there exists a finite quadratic transform $z(R)$ of R such that the birational correspondence between $z(R)$ and $y(R)$ is regular at every point in $\bar{z}(R)$.*

Proof. Since in this case every point in $\bar{z}^{(\pi)}(R)$ must have a dimension over $\bar{R}$ which is either $t-1$ or $t-2=0$, it follows from the proof above that T_π is regular at every point in $\bar{z}^{(\pi)}(R)$. We can therefore take $z(R)$ to be $z^{(\pi)}(R)$.

Corollary 2. *The topological space $\mathfrak{V}(R)$ is connected.*

This follows immediately from Theorem 1 and the definition of topology in $\mathfrak{V}(R)$ given in section 2.

4. General connectedness theorem and extended principle of Degeneration. We begin by recalling the well-known Hensel's Lemma: If a splitting form $F(X)$ with coefficients in a complete real discrete valuation ring R is irreducible over R (or over the quotient field K of R, which in this case amounts to the same thing), then the residue form $\bar{F}(X)$, if it does not vanish identically, is not the product of two relatively prime forms in $\bar{R}[X]$. Geometrically, this means that if a positive 0-cycle Z is rational and irreducible over K, then its specialization $\bar{Z}(R)$ at R is $\bar{R}$-connected. Our purpose here is to generalize this Hensel's Lemma to the case where R is an arbitrary complete local domain. In a sense something of this nature has already been done in the literature; in fact, it is well-known that the Hensel's Lemma, at least in the case of a form of two variables, holds for any complete local ring R (see e. g. [6], Theorem 4), for the usual proof of the Hensel's Lemma

for a valuation ring can be carried over without any difficulties to the general case. However, this generalization is essentially a trivial one and in reality deals only with a highly specialized situation; for the condition that the residue form $\bar{F}(X)$ does not vanish identically, while easily obtainable in case of a valuation ring by a suitable choice of the factor of proportionality, imposes a very severe restriction on the form $F(X)$ in the general case. Expressed in geometrical terms, this condition means that the cycle Z must have a uniquely determined specialization at R, so that the set $\bar{Z}(R)$ consists of only a single cycle; while this is always true in case of a valuation ring, it evidently represents a severe restriction in the general case. In fact, the fact that $\bar{Z}(R)$ is in general an algebraic set of cycles instead of a single cycle, can be considered as the principal new feature in local algebraic geometry which one encounters in going over from valuation rings to arbitrary local domains. A true generalization of the Hensel's Lemma should therefore take account of this important point, and in lieu of the $\bar{R}$-connectedness of a single residue cycle, it should supply us with some information about the $\bar{R}$-connectedness properties of the entire set of cycles $\bar{Z}(R)$. The General Connectedness Theorem, as formulated in § 1, is a theorem of just such a nature and can therefore very appropriately be considered as a generalization of the Hensel's Lemma, or rather, since it deals with cycles of arbitrary dimensions, as a generalization of the Principle of Degeneration as formulated and proved in [4], which is itself a generalization of the Hensel's Lemma to cycles of higher dimensions while retaining the assumption of a valuation ring. However, it is possible to formulate a theorem which is an even truer generalization of the Principle of Degeneration in the sense that it deals with the $\bar{R}$-connectedness properties not of the point set $|\bar{Z}(R)|$, but rather of the individual cycles in $\bar{Z}(R)$. This leads us to what we shall call the Extended Principle of Degeneration, from which one can easily obtain the General Connectedness Theorem as a simple corollary, as we have already mentioned in § 1.

We shall speak of a *continuous system* of positive r-cycles in $\bar{S}^n$ *parametrized* by a local domain R, if there is a continuous mapping $N \to \Xi(N)$ $(N \in \mathfrak{V}(R))$ of the set $\mathfrak{V}(R)$ of all valuation rings in K dominating R into the set $\mathfrak{Z}(\bar{S}^n)$ of all positive r-cycles in $\bar{S}^n$ such that for every N the cycle $\Xi(N)$ is rational over thet residue field $\bar{N}$ of N. We shall denote such a continuous system of cycles by the symbols $\Xi(R)$. The continuity condition here in the definition refers to the Zariski $\bar{R}$-topologies of both $\mathfrak{V}(R)$ and $\mathfrak{Z}(\bar{S}^n)$; we recall that the topology of $\mathfrak{V}(R)$ is defined by means of the system of Zariski $\bar{R}$-topologies of the centers of all rational transforms of R, as described after Lemma 2. 2 in section 2, while the topology of $\mathfrak{Z}(\bar{S}^n)$ is that of the

(discrete) union of an infinite sequence of spaces, each one of which is the set of all positive r-cycles of a given degree in $\bar{S}^n$ and is being endowed with its Zariski $\bar{R}$-topology by means of the associated points. In particular, this implies that if N and N' are two elements in $\mathfrak{V}(R)$ such that N' is the quotient ring of N, then $\Xi(N)$ is a specialization of $\Xi(N')$ over $\bar{R}$. In terms of the associated forms, the continuous system of cycles $\Xi(R)$ can be given by a *continuous system* of forms $\Phi_R(U) = \{\Phi_N(U) \mid N \in \mathfrak{V}(R)\}$ such that each $\Phi_N(U)$ is an associated form and is rational over $\bar{N}$, whereby we observe that these forms are determined only up to proportionality factors and that rationality of a form refers to the ratios of the coefficients.

Let R_1 be a local domain dominating R, not necessarily contained in the quotient field K of R; since every valuation ring in the quotient field of R_1 dominating R_1 contracts in K to a valuation ring dominating R, there is defined in this way a canonical mapping of $\mathfrak{V}(R_1)$ into $\mathfrak{V}(R)$, which is easily seen to be continuous. If we set $\Xi(N) = \Xi(K \cap N)$ for every N in $\mathfrak{V}(R_1)$, then the mapping $N \to \Xi(N)$ $(N \in \mathfrak{V}(R_1))$ defines evidently a continuous system parametrized by R_1, which we shall denote by $\Xi(R_1)$ and call the *subsystem* of $\Xi(R)$ determined by R_1.

We remark that in general the cycles in a continuous system $\Xi(R)$ can very well have different degrees; in particular, for some N the cycle $\Xi(N)$ may have the degree 0, i.e. $\Xi(N)$ is the zero r-cycle. If every cycle in a continuous system has the degree 0, so that all of them coincide with the zero r-cycle, then the system is said to be *trivial*. However, in the important case where $\mathfrak{V}(R)$ is connected, as is the case with a regular local ring R according to Theorem 1, Corollary 2, it can be easily seen that all cycles in a continuous system $\Xi(R)$ must have the same degree, so that if for any one N the cycle $\Xi(N)$ has the degree 0, then the system $\Xi(R)$ must be trivial. To see this, one need only to observe that the set of all positive cycles of a given degree d in $\bar{S}^n$ is a closed subset in $\mathfrak{Z}(\bar{S}^n)$ and so is the set of all positive cycles in $\bar{S}^n$ of degrees different from d; the inverse images of these two subsets under the mapping $N \to \Xi(N)$ must then be two disjoint closed subsets in $\mathfrak{V}(R)$ whose union coincides with $\mathfrak{V}(R)$, and hence one of them must be empty. This means that if d is the degree of any one cycle in $\Xi(R)$, then all the other cycles in $\Xi(R)$ must have the same degree d.

If there exist two non-trivial continuous systems of positive r-cycles $\Xi'(R)$ and $\Xi''(R)$ such that we have the equation $\Xi(N) = \Xi'(N) + \Xi''(N)$ for every N in $\mathfrak{V}(R)$, then we shall say that the system $\Xi(R)$ *splits* into the two systems $\Xi'(R)$ and $\Xi''(R)$, or that the pair $(\Xi'(R), \Xi''(R))$ is a splitting of $\Xi(R)$. Such a splitting is said to be $\bar{R}$-disjoint at a valuation ring N if

$\Xi'(N)$ and $\Xi''(N)$ are $\bar{R}$-disjoint, i.e. the supports of $\Xi'(N)$ and $\Xi''(N)$ are disjoint sets in the Zariski $\bar{R}$-topology, and it is said to be *everywhere $\bar{R}$-disjoint* or simply *$\bar{R}$-disjoint* if it is $\bar{R}$-disjoint at every N in $\mathfrak{V}(R)$. In terms of the associated forms, a splitting of $\Xi(R)$ can be given by a splitting of the system of forms $\Phi_R(U)$ into two systems of forms $\Phi'_R(U)$ and $\Phi_R''(U)$, so that for every N in $\mathfrak{V}(R)$ we have the equation $\Phi_N(U) \doteq \Phi'_N(U)\Phi''_N(U)$, where the symbol $\doteq$ denotes equality up to proportionality factors; and we observe that in case $r = 0$, the cycles $\Xi'(N)$ and $\Xi''(N)$ are $\bar{R}$-disjoint if and only if their associated forms $\Phi'_N(U)$ and $\Phi''_N(U)$ are relatively $\bar{R}$-prime, i.e. there does not exist a splitting form in $\bar{R}[U]$ which has common factors with both $\Phi'_N(U)$ and $\Phi''_N(U)$. Finally, a continuous system of cycles is said to be *$\bar{R}$-connected* if it does not have any $\bar{R}$-disjoint splitting.

If Z is a positive r-cycle in S^n, rational over K, then the algebraic set of cycles $\bar{Z}(R)$ forms in a natural way a continuous system parametrized by R, which we shall also denote by the same symbol $\bar{Z}(R)$, there being not much danger of confusion on this score. In this case, we shall say that the cycle Z *generates* the continuous system $\bar{Z}(R)$. If the cycle Z is the sum of two positive r-cycles Z' and Z'', also rational over K, then it is clear that we have the equation $\bar{Z}(N) = \bar{Z}'(N) + \bar{Z}''(N)$ for every N in $\mathfrak{V}(R)$; hence the system $\bar{Z}(R)$ splits into the two systems $\bar{Z}'(R)$ and $\bar{Z}''(R)$. Thus we see that a splitting of the cycle Z induces a splitting of the system $\bar{Z}(R)$ generated by Z. The Extended Principle of Degeneration, which we shall now formulate, asserts that conversely every $\bar{R}$-disjoint splitting of the system $\bar{Z}(R)$ can be obtained in this way. We shall prove this principle here only for the case of a complete regular local ring, although it is very likely that it holds generally for an arbitrary complete local domain.

THEOREM 2 (Extended Principle of Degeneration). *Let $(R, \mathfrak{p})$ be a complete regular local ring, with the quotient field K and the residue field $\bar{R}$, and let Z be a positive cycle in S^n, rational over K; if Z is K-connected, then the continuous system of cycles $\bar{Z}(R)$ is $\bar{R}$-connected.*

The proof of this theorem will be given in the next section. Here we shall show how the General Connectedness Theorem can be obtained from it by a very simple argument.

THEOREM 3 (General Connectedness Theorem). *Let $(R, \mathfrak{p})$ be a complete local domain, with the quotient field K and the residue field $\bar{R}$, and let Z be a positive cycle in S^n, rational over K; if Z is K-connected, then the point set $|\bar{Z}(R)|$ is $\bar{R}$-connected.*

Proof. In case R is regular, this theorem follows almost immediately from Theorem 2. In fact, if there exist two disjoint $\bar{R}$-closed subsets Ω' and Ω'' in $\bar{S}^n$ such that $|\bar{Z}(R)|$ is contained in their union and has non-empty intersections with both of them, and if we denote by $\Xi'(N)$ and $\Xi''(N)$ the restriction of $\bar{Z}(N)$ in Ω' and Ω'' respectively, then we obtain two continuous systems $\Xi'(R)=\{\Xi'(N)\mid N\in\mathfrak{V}(R)\}$ and $\Xi''(R)=\{\Xi''(N)\mid N\in\mathfrak{V}(R)\}$ which are clearly non-trivial, and the equation $\bar{Z}(N)=\Xi'(N)+\Xi''(N)$ defines evidently an $\bar{R}$-disjoint splitting of the system $\bar{Z}(R)$ into the two systems $\Xi'(R)$ and $\Xi''(R)$; it follows then from Theorem 2 that Z cannot be K-connected. It remains to show that the general case of an arbitrary complete local domain can be reduced to this special case.

According to Cohen [6], Theorem 16, there exists a subring R_0 in R such that R_0 is a complete regular local ring having the same dimension and the same residue field as R, and such that R is a finite module over R_0; this implies that K is a finite algebraic extension of the quotient field K_0 of R_0. Let $Z_1=Z, Z_2,\cdots,Z_s$ be the complete set of conjugates of Z over K_0, and let $K_1=K, K_2,\cdots,K_s$ and $R_1=R, R_2,\cdots,R_s$ be the corresponding sets of conjugates of K and R respectively over K_0; let K' be the compositum of all K_i and let R' be the ring generated by all the R_i. Since R' is a finite module over R_0 and since R_0 is complete, it follows from [3], III, Proposition 8, that R' is a complete local domain; since the local rings R_i all have the same residue field $\bar{R}$, we can attach R' to Λ by identifying its residue field also with $\bar{R}$, so that R' dominates all R_i as well as R_0. Furthermore, it is easily seen that for any valuation ring in K_0 dominating R_0, any extension of it in K' must dominate R'; and a similar statement holds also for valuation rings in K_i dominating R_i. We set $Z_0=\sum_{i=1}^{s} Z_i$, so that Z_0 is rational over K_0; since Z is K-connected, it follows that Z_0 is K_0-connected. In fact, any K_0-irreducible component X_0 in Z_0 is the sum of the complete set of conjugates over K_0 of a K-irreducible component X in Z, and two such components X_0 and Y_0 in Z_0 will certainly meet if the corresponding components X and Y in Z meet. It is sufficient to show that $|\bar{Z}_0(R_0)|=|\bar{Z}(R)|$; for, since R_0 is a complete regular local domain, $|\bar{Z}_0(R_0)|$ must be $\bar{R}$-connected by what we have just shown above, and hence $|\bar{Z}(R)|$ must also be $\bar{R}$-connected.

Since every valuation ring in K_0 dominating R_0 can be extended to a valuation ring in K' dominating R', it follows that $\bar{Z}_0(R_0)=\bar{Z}_0(R')$, and since every valuation ring in K_i dominating R_i can also be extended to a valuation ring in K' dominating R', it follows that $\bar{Z}_i(R_i)=\bar{Z}_i(R')$. It is sufficient to show that $|\bar{Z}(R)|=|\bar{Z}_i(R_i)|$ for every i; for then $|\bar{Z}_0(R_0)|$

$= |\bar{Z}_0(R')| = \bigcup_i |\bar{Z}_i(R')| = \bigcup_i |\bar{Z}_i(R_i)| = |\bar{Z}(R)|$. To prove this we observe first that R_0 contains a coefficient ring k ([6], Theorem 9 and Theorem 11) which is also a coefficient ring for every R_i and is invariant under the isomorphism between R and R_i over R_0. Let a and a' be any two conjugate elements over K_0 in R and R_i respectively, and let b be an element in k such that $\bar{b} = \bar{a}$ (such an element b exists by the definition of a coefficient ring); then $a - b$ is in $\mathfrak{p}$, and hence by isomorphism $a' - b$ is in $\mathfrak{p}_i$ (the maximal prime ideal in R_i), which show that $\bar{b} = \bar{a}'$. Thus any two conjugate elements over K_0 in R and R_i must have the same residue in $\bar{R}$. Let y be the associated point of Z, and let y' be the associated point of Z_i; if $f(Y)$ and $f'(Y)$ are two conjugate forms over K_0 in $R[Y]$ and $R_i[Y]$ respectively, then by isomorphism we have the relation $f(y) = 0$ if and only if $f'(y') = 0$, and it follows from what we have just shown that the residue forms $\bar{f}(Y)$ and $\bar{f}'(Y)$ must coincide. Since $\bar{y}(R)$ and $\bar{y}'(R_i)$ are defined by such residue forms, it follows that the two sets $\bar{y}(R)$ and $\bar{y}'(R_i)$ must coincide; hence the two algebraic sets of cycles $\bar{Z}(R)$ and $\bar{Z}_i(R_i)$ must coincide, and hence $|\bar{Z}(R)| = |\bar{Z}_i(R_i)|$.

We observe here that if we are only concerned with the absolute geometry and assume the absolute connectednesss of Z, then it would be sufficient to invoke the simpler Principle of Degeneration in [4] instead of Theorem 2; only we must then invoke directly the connectedness of $\mathfrak{V}(R)$, which will also be used in the proof of Theorem 2. In fact, in this case Z would be N^*-connected for every N in $\mathfrak{V}(R)$, and therefore by that principle $\bar{Z}(N^*) = \bar{Z}(N)$ would be $\bar{N}$-connected and hence also $\bar{R}$-connected. Then, instead of using Theorem 2, we need only to observe in the first part of the above proof that since $\mathfrak{V}(R)$ is connected, all cycles in each of the systems $\Xi'(R)$ and $\Xi''(R)$ must have the same degree, so that every cycle in $\bar{Z}(R)$ must split into two $\bar{R}$-disjoint parts. Of course, since in this case the hypothesis is preserved under any extension of the local domain R to another complete local domain dominating it, one sees readily that the point set $|\bar{Z}(R)|$ must in fact be absolutely connected.

We shall conclude this section with a remark on the uniqueness of the type of splittings which arise from the Hensel's Lemma. Let R be a valuation ring in a field K, with the residue field $\bar{R}$, and let $F(X)$ be a form in $R[X]$; if $F(X) = G(X)H(X)$ is a splitting of $F(X)$ in $R[X]$ (or in $K[X]$) such that $\bar{G}_R(X)$ and $\bar{H}_R(X)$ are relatively prime forms in $\bar{R}[X]$, then $G(X)$ and $H(X)$ are uniquely determined by the forms $\bar{G}_R(X)$ and $\bar{H}_R(X)$ up to proportionality factors in K. Therefore, if a, b, c are the *leading coefficients* (leading coefficient = coefficient of the term with the lowest "weight") in

$F(X)$, $G(X)$, $H(X)$ respectively, then the additional stipulation of the splitting $a = bc$ in R or K determines the forms $G(X)$ and $H(X)$ uniquely. For proof, one need only observe that since $\bar{G}_R(X)$ and $\bar{H}_R(X)$ are relatively prime, $G(X)$ and $H(X)$ must also be relatively prime, and the uniqueness of the splitting $F(X) = G(X)H(X)$ then follows from the unique factorization property of the polynomial ring $K[X]$. It is convenient to express this uniqueness by saying that the splitting $F(X) = G(X)H(X)$ is determined uniquely by the *initial condition* $(\bar{G}_R(X), \bar{H}_R(X); b, c)$.

5. Proof of Theorem 2. We shall first prove a lemma on a relation between a complete regular local ring and the completion of its quadratic valuation ring.

Let $(R, \mathfrak{p})$ be a complete regular local ring of dimension t, with the quotient field K and the residue field $\bar{R}$, and let $x_1, \cdots, x_t$ be the elements in a minimal basis for $\mathfrak{p}$. We denote by Q a system of representatives of $\bar{R}$ in R; apart from the condition that every element in $\bar{R}$ is the $\mathfrak{p}$-residue of exactly one element in Q, the elements in Q can be chosen arbitrarily, but for convenience we shall assume that Q contains the elements 0 and 1. We denote by $Q[x] = Q[x_1, \cdots, x_t]$ the set of all polynomials in $x_1, \cdots, x_t$ with coefficients in Q, and we shall say that an element in $Q[x]$ is *monic* if the coefficient of the leading term (i.e. the term with the lowest weight, each x_i being assigned the weight i) is 1. We denote by $Q(x)$ the set of all quotients $f(x)/g(x)$ of two elements in $Q[x]$ such that $g(x)$ is monic and that the polynomials $\bar{f}(T)$ and $\bar{g}(T)$ are relatively prime (where $T = (T_1, \cdots, T_t)$ is a system of indeterminates), and we shall say that an element $f(x)/g(x)$ in $Q(x)$ is homogeneous of degree i if both $f(x)$ and $g(x)$ are forms in x and $i =$ degre of $f(x)$ — degree of $g(x)$. We shall now associate with the system of elements $x = (x_1, \cdots, x_t)$ a system of independent variables $\boldsymbol{x} = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t)$ over $\bar{R}$ in Λ; then we can associate with each element $f(x)/g(x)$ in $Q(x)$ the element $\bar{f}(\boldsymbol{x}/\bar{g}(\boldsymbol{x})$ in the field $\bar{R}(\boldsymbol{x})$, which we shall call the *homogeneous residue* of $f(x)/g(x)$. It is easily seen that, by virtue of our choice of the elements in $Q(x)$ made above, this association of the elements in $Q(x)$ with their homogeneous residues in $\bar{R}(\boldsymbol{x})$ is a one-to-one mapping of $Q(x)$ onto $\bar{R}(\boldsymbol{x})$, which maps the subset $Q[x]$ onto the subring $\bar{R}[\boldsymbol{x}]$.

We denote by $Q[(x)]$ the set of all series of the type $\sum_{i=0}^{\infty} a^{(i)}$, where each term $a^{(i)}$ is a homogeneous element of degree i in $Q(x)$, and we denote by $Q[[x]]$ the subset in $Q[(x)]$ consisting of all such series in which each term

$a^{(i)}$ is a homogeneous degree i in $Q[x]$. Now, since R is a complete regular local ring, it can be easily shown that every element a in R can be represented *in a unique manner* by a series $a = \sum_{i=0}^{\infty} a^{(i)}$ in $Q[[x]]$, while conversely it is obvious that any series in $Q[[x]]$ is convergent in the topology of R and hence represent an element in R; this shows that we can set $R = Q[[x]]$, and we shall say that the series $\sum_{i=0}^{\infty} a^{(i)}$ is the *power series development* of the element a (with respect to the given choice of the basis elements $x_1, \cdots, x_t$ and the system Q), although it is in general not a power series in the usual sense. Similarly, if we denote by $(M, \mathfrak{q})$ the $\mathfrak{p}$-adic valuation ring of R, then every element in the completion M^* of M can be represented *in a unique manner* by a series in $Q[(x)]$, while conversely it is also obvious from the definition of the $\mathfrak{p}$-adic valuation that any series in $Q[(x)]$ is convergent in the topology of M and hence represent an element in M^*; therefore we can set $M^* = Q[(x)]$, and we shall say that the series in $Q[(x)]$ corresponding to an element in M^* is the *power series development* of this element.

If $a = \sum_{i=0}^{\infty} a^{(i)}$ is any element in M^*, then the first non-zero term $a^{(\mu)}$ in the series is called the *initial element* of a and the number μ is called the *order* of a; the homogeneous residue $\boldsymbol{a}^{(\mu)}$ of $a^{(\mu)}$ is also called the homogeneous residue of a and will be denoted also by $\boldsymbol{a}$. For elements of order zero in M^*, i.e. units in M^*, the mapping $a \rightarrow \boldsymbol{a}$ induces an isomorphism between the residue field $M^*/M^*\mathfrak{q}$ and the subfield in $\bar{R}(\boldsymbol{x})$ consisting of all homogeneous elements of order zero; we can therefore attach M^* to Λ by identifying $M^*/M^*\mathfrak{q}$ with this subfield, and we observe that with this attachment of M^* the homogeneous residue $\boldsymbol{a}$ of any element a of order zero coincides with its residue $\bar{a}$ modulo $M^*\mathfrak{q}$. Geometrically, we can consider the system $\boldsymbol{x} = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t)$ as the system of homogeneous coordinates of a generic point ζ over $\bar{R}$ of the center $\bar{x}(R)$ of the quadratic transform $x(R)$ of R, so that we can set $\bar{R}(\zeta) = M/\mathfrak{q} = M^*/M^*\mathfrak{q}$. However, we stress here that the elements $\boldsymbol{x}_i$ are not in $\bar{R}(\zeta)$, and that the symbol $\boldsymbol{x}$ denotes the system of t elements $(\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t)$, not the point ζ, whose homogeneous coordinates are after all only determined up to a proportionality factor.

If $F(X)$ is a polynomial (or form) in $M^*[X] = M^*[X_0, X_1, \cdots, X_n]$, then we can consider the *power series development* $F(X) = \sum_{i=0}^{\infty} F^{(i)}(X)$, where $F^{(i)}(X)$ is a polynomial (or form) in X with coefficients which are homogeneous elements of degree i in $Q(x)$; the first non-vanishing term $F^{(\lambda)}(X)$

in this series is then called the *initial polynomial* (or *form*) of $F(X)$, and the polynomial (or form) $\boldsymbol{F}^{(\lambda)}(X)$ obtained from $F^{(\lambda)}(X)$ by replacing every coefficient in it by its homogeneous residue will be called the *homogeneous residue polynomial* (or *form*) of $F(X)$ and will be denoted also by $\boldsymbol{F}(X)$. it is clear that in case $F^{(0)}(X)$ does not vanish, we have the equation $\boldsymbol{F}(X) = \boldsymbol{F}^{(0)}(X) = \bar{F}(X)$.

Let η be a point of dimension $t - s$ over $\bar{R}$ in the center $\bar{x}(R)$ of the quadratic transform $x(R)$; without any loss of generality, we can assume that $\eta_1 = 1$ and that $\eta_{s+1}, \cdots, \eta_t$ are independent variables over $\bar{R}$. Since $\bar{x}(R)$ coincides with the projective space $\bar{S}^{t-1}$, there exist $s - 1$ forms $\phi_2(X), \cdots, \phi_s(X)$ in $\bar{R}[X]$ of the same degree μ such that the elements $\phi_2(\zeta)/\zeta_1{}^{\mu}, \cdots, \phi_s(\zeta)/\zeta_1{}^{\mu}$ constitute a basis for the maximal prime ideal in the specialization ring $\mathfrak{Q}(\zeta/\eta, \bar{R})$ in $\bar{R}(\zeta)$ of $\bar{S}^{t-1}$ at η. If $f_2(X), \cdots, f_s(X)$ are forms in $R[X]$ such that $\bar{f}_i(X) = \phi_i(X)$, then the elements $x'_1 = x_1$, $x'_2 = f_2(x)/x_1{}^{\mu-1}, \cdots, x'_s = f_s(x)/x_1{}^{\mu-1}$ constitute a basis for the maximal prime ideal in $\mathfrak{Q}(x(R)/\eta)$. Since η is a specialization of ζ over $\bar{R}$, M is the quotient ring of $\mathfrak{Q}(x(R)/\eta)$ with respect to the prime ideal $\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}$, and since the ideal $\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}$ must then have the rank 1 and evidently contains the prime ideal generated by $x'_1 = x_1$ in $\mathfrak{Q}(x(R)/\eta)$, it must coincide with the latter. Furthermore, it is easily seen that $\mathfrak{Q}(x(R)/\eta)/\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}$ is isomorphic to $\mathfrak{Q}(\zeta/\eta, \bar{R})$ and hence can be identified with the latter, so that $M/\mathfrak{q} = \bar{R}(\zeta)$ is the quotient field of $\mathfrak{Q}(x(R)/\eta)/\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}$.

Consider now the completion $(R_1, \mathfrak{p}_1)$ of $\mathfrak{Q}(x(R)/\eta)$ and denote by $\mathfrak{q}_i$ the prime ideal generated by x'_1 in R_1 (note that x'_1 is also an element of a basis for $\mathfrak{p}_1$); since $\mathfrak{q}_1 = R_1(\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q})$, it follows that $R_1/\mathfrak{q}_1$ is the completion of $\mathfrak{Q}(x(R)/\eta)/\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q} = Q(\zeta/\eta, \bar{R})$. Let $(M', \mathfrak{q}')$ be the quotient ring of R_1 with respect to $\mathfrak{q}_1$, which is a real discrete valuation ring. Since M is the quotient ring of $\mathfrak{Q}(x(R)/\eta)$ with respect to $\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q} = \mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}'$, it can be embedded canonically as a subring in M', and if we attach M' to Λ compatibly with the attachement of M to Λ, then it is clear that M' dominates M. Consider now the completion M'^* of M'; it is important for our present purpose to observe that the completion M^* of M *can be embedded canonically in M'^* as a subspace.* In fact, according to [12], Lemma 7, we have the relation $R_1 \cap \mathfrak{q}'^i = R_1(\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}^i)$ for every positive integer i; it follows that

$$\begin{aligned}\mathfrak{Q}(x(R)/\eta) \cap (M \cap \mathfrak{q}'^i) &= \mathfrak{Q}(x(R)/\eta) \cap (R_1 \cap \mathfrak{q}'^i)\\ &= \mathfrak{Q}(x(R)/\eta) \cap R_1(\mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}^i) = \mathfrak{Q}(x(R)/\eta) \cap \mathfrak{q}^i,\end{aligned}$$

and hence $M \cap \mathfrak{q}'^i = \mathfrak{q}^i$. This shows that M' contains M as a subspace, and hence M'^* contains M^* as a subring.

Let $a = \sum_{i=\lambda}^{\infty} a^{(i)}$ be an element in M^*, expressed as a power series with $a^{(\lambda)} \neq 0$. We want to find the condition that this element a be contained in R_1; this question makes sense because both M^* and R_1 are subrings in M'^*. It is evidently sufficient to assume that every element $a^{(i)}$ is contained in $\mathfrak{Q}(x(R)/\eta)$; we shall show that this condition is also necessary. If a is contained in R_1, then $a/x_1{}^\lambda$ is also contained in R_1; hence the $M'^*\mathfrak{q}'$-residue of $a/x_1{}^\lambda$, being also the $\mathfrak{q}_1$-residue of $a/x_1{}^\lambda$, is contained in the completion of $\mathfrak{Q}(\zeta/\eta, \bar{R})$. On the other hand, since $a/x_1{}^\lambda$ and $a^{(\lambda)}/x_1{}^\lambda$ have the same $M'^*\mathfrak{q}'$-residue, and since the $M'^*\mathfrak{q}'$-residue of $a^{(\lambda)}/x_1{}^\lambda$, being also the $\mathfrak{q}$-residue of $a^{(\lambda)}/x_1{}^\lambda$, is contained in $\bar{R}(\zeta)$, it follows that the $M'^*\mathfrak{q}'$-residue of $a^{(\lambda)}/x_1{}^\lambda$ must be contained in both $\bar{R}(\zeta)$ and the completion of $\mathfrak{Q}(\zeta/\eta, \bar{R})$. Since $\bar{R}(\zeta)$ is the quotient field of $\mathfrak{Q}(\zeta/\eta, \bar{R})$, it follows from a well-known property of local rings that the $M'^*\mathfrak{q}'$-residue of $a^{(\lambda)}/x_1{}^\lambda$ must be contained in $\mathfrak{Q}(\zeta/\eta, \bar{R})$. Since this means that the $\mathfrak{q}$-residue of $a^{(\lambda)}/x_1{}^\lambda$ is contained in $\mathfrak{Q}(\zeta/\eta. \bar{R})$, it follows from the uniqueness of the power series development of a that $a^{(\lambda)}/x_1{}^\lambda$ must be contained in $\mathfrak{Q}(x(R)/\eta)$, and hence $a^{(\lambda)}$ itself must be contained in $\mathfrak{Q}(x(R)/\eta)$. Now since the element $a - a^{(\lambda)}$ is also an element in R_1, we can apply the same argument to it as we did to a and conclude that $a^{(\lambda+1)}$ must also be contained in $\mathfrak{Q}(x(R)/\eta)$. Thus, continuing in this way, we conclude that every element $a^{(i)}$ is contained in $\mathfrak{Q}(x(R)/\eta)$.

Since R is the intersection of all the rings $\mathfrak{Q}(x(R)/\eta)$ as η runs through all points in $\bar{x}(R)$ (in fact, it is sufficient to consider only point of dimension $t-2$ over $\bar{R}$), it follows that an element in M^* is in R if and only if it is contained in the completion of $\mathfrak{Q}(x(R)/\eta)$ for every point η (of dimension $t-2$ over $\bar{R}$) in $\bar{x}(R)$. We shall state this result as a lemma for later reference.

LEMMA 5.1. *An element in M^* is in R if and only if it is contained in the completion of $\mathfrak{Q}(x(R)/\eta)$ for every point η (of dimension $t-2$ over $\bar{R}$) in $\bar{x}(R)$.*

Consider now the canonical mapping of M'^* onto $M'^*/\mathfrak{q}'^* = M'/\mathfrak{q}'$, and let M_1 be the subring in M'^* consisting of all elements whose images under this mapping are in $R_1/\mathfrak{q}_1$; it is clear that M_1 contains $\mathfrak{q}'^*$ as a minimal prime ideal, and that $M_1/\mathfrak{q}'^* = R_1/\mathfrak{q}_1$ and $M_{1,\mathfrak{q}'^*} = M'^*$. In case $t = s = 2$, the local ring $R_1/\mathfrak{q}_1$ has the dimension 1 and hence is a complete real discrete valuation ring; it follows then that in this case M_1 is a discrete valuation ring of rank 2,

obtained from the composition of the valuations of M'^* and $R_1/\mathfrak{q}_1$, and that it is complete. This ring M_1 will be useful to us later; we observe here that M_1 dominates R_1.

We proceed now to prove Theorem 2.

Proof of Theorem 2. We observe first that, just as in the proof of the Principle of Degeneration in [4], we can without any loss of generality restrict ourselves to the case where Z is K-irreducible. For the condition for the supports of two positive cycles to have a common point can be expressed by a system of "universal" equations in the coefficients of their associated forms, and it is clear that such a condition is always preserved under a specialization. If Z is the sum of two positive cycles Z' and Z'', both rational over K, such that their supports meet, then the support of $\bar{Z}'(N)$ and $\bar{Z}''(N)$ must also meet for every N in $\mathfrak{V}(R)$, so that $\bar{Z}'(N)$ and $\bar{Z}''(N)$ cannot be $\bar{R}$-disjoint; it follows then that any $\bar{R}$-disjoint splitting of the system $\bar{Z}(R)$ will induce an $\bar{R}$-disjoint splitting of at least one of the two systems $\bar{Z}'(R)$ and $\bar{Z}''(R)$. Thus the validity of our theorem for every K-irreducible positive cycle will imply its validity in the general case.

Next, we show that we can reduce our theorem to the special case where Z is a positive 0-cycle. Let $u^{(i)}{}_j$, $i=1,\cdots,r$, $j=0,1,\cdots,n$, be $r(n+1)$ independent variables over K, and set $u^{(i)}=(u^{(i)}{}_0,u^{(i)}{}_1,\cdots,u^{(i)}{}_n)$, $i=1,\cdots,r$ (r being the dimension of the cycle Z). The ring $R[[u]]$ of all power series in $u^{(i)}{}_j$ with coefficients in R is easily seen to be a complete regular local ring (of dimension $t+r(n+1)$, t being the dimension of R), and we can attach it to Λ by identifying the residue field of $R[[u]]$ with $\bar{R}$, so that $R[[u]]$ dominates R. Let $F(U^{(0)},U^{(1)},\cdots,U^{(r)})$ be the associated form of Z, and consider the form $F(U^{(0)},u)=F(U^{(0)},u^{(1)},\cdots,u^{(r)})$ obtained from it by substituting the indeterminates $U^{(1)},\cdots,U^{(r)}$ by $u^{(1)},\cdots,u^{(r)}$; it is clear that since $F(U^{(0)},U^{(1)},\cdots,U^{(r)})$ is K-irreducible, $F(U^{(0)},u)$ must be $K(u)$-irreducible. Since the coefficients in $F(U^{(0)},u)$ are homogeneous of the same degree in the variables $u^{(i)}{}_j$, it is easily seen that $F(U^{(0)},u)$ must be irreducible also over the power series ring $K[[u]]$; and since $K[[u]]$ is a unique-factorization ring, this implies that $F(U^{(0)},u)$ is irreducible over the quotient field $K((u))$ of $K[[u]]$, and hence also irreducible over the quotient field $R((u))$ of $R[[u]]$. The form $F(U^{(0)},u)$ therefore determines a positive 0-cycle Z_u in S^n which is rational and irreducible over $R((u))$; and we observe that since Z_u is contained in the support of Z, the cycle $\bar{Z}_u(N_1)$ must be contained in the support of the cycle $\bar{Z}(N_1)$ for every valuation ring N_1 in $\mathfrak{V}(R[[u]])$. If $\bar{Z}(N)=\Omega'(N)+\Omega''(N)$ $(N\in\mathfrak{V}(R))$ is an $\bar{R}$-disjoint splitting of $\bar{Z}(R)$, then we denote by $\Omega'_u(N_1)$ and $\Omega''_u(N_1)$ the restrictions of

$\bar{Z}_u(N_1)$ in $|\Omega'(N_1)|$ and $|\Omega''(N_1)|$ respectively; the equation $Z_u(N_1) = \Omega'(N_1) + \Omega''_u(N_1)$ $(N_1 \in \mathfrak{V}(R[[u]]))$ then defines an $\bar{R}$-disjoint splitting of $\bar{Z}_u(N_1)$, provided it is not trivial for at least one N_1. But this is easily seen to be the case when we take for N_1 the quadratic valuation ring of $R[[u]]$; for in this case $\bar{u}^{(i)}(N_1)$, $i=1,\cdots,r$, are independent generic points in S^n over a field of rationality for $\bar{Z}(N_1)$, and $\bar{Z}_u(N_1)$ is simply the intersection cycle of $\bar{Z}(N_1)$ with the linear subspace of dimension $n-r$ defined by the r dual hyperplanes of the points $\bar{u}^{(i)}(N_1)$. Thus the validity of our theorem for the 0-cycle Z_u implies its validity for the r-cycle Z.

Finally, we reduce our theorem to the case where the dimension t of R is equal to 2, whereby we note that the case $t=1$ (Z being now a 0-cycle) reduces essentially to the Hensel's Lemma. We observe first that it is permissible to replace R by the complete local domain $R(v)^*$ obtained from R by the adjunction of $t-2$ independent variables $v=(v_1,\cdots,v_{t-2})$ over K; for the cycle Z will remain irreducible over $K(v)$, while any $\bar{R}$-disjoint splitting of $\bar{Z}(R)$ will induce an $\bar{R}(\bar{v})$-disjoint splittings of $\bar{Z}(R(v)^*)$ through the mapping $N \rightarrow N \cap K$ of $\mathfrak{V}(R(v)^*)$ into $\mathfrak{V}(R)$. We can therefore apply Lemma 2.9 (taking $d=t-2$) and consider the local domain R_v^* introduced there, which is a complete regular local ring of dimension 2; since K is algebraically closed in the quotient field of R_v^* and Z is irreducible over K, it follows that Z is also irreducible over the quotient field of R_v^*. On the other hand, since R_v^* dominates R, the system $\bar{Z}(R_v^*)$ is a subsystem of $\bar{Z}(R)$; it follows that an $\bar{R}$-disjoint splitting of $\bar{Z}(R)$ will induce also such a splitting of $\bar{Z}(R_v^*)$; which must be of course also $\bar{R}(\bar{v},\bar{u})$-disjoint, using the notation in Lemma 2.9. Thus the validity of our theorem for the case $r=0$, $t=2$, will imply its validity in the general case.

We therefore have to prove our theorem only for the case where Z is a K-irreducible positive 0-cycle and R is a complete regular local ring of dimension 2; we assume that there exists an $\bar{R}$-disjoint splitting of the system $\bar{Z}(R)$ and we shall show that the cycle Z must then be reducible over K, in contradiction to our hypothesis. In terms of the associated form $F(U)$, the given $\bar{R}$-disjoint splitting of $\bar{Z}(R)$ can be expressed by a splitting $\bar{F}_N(U) \doteq \Phi_N(U)\Theta_N(U)$ of the system of forms $\bar{F}_R(U)$ into two systems $\Phi_R(U)$ and $\Theta_R(U)$ such that $\Phi_N(U)$ and $\Theta_N(U)$ are relatively prime over $\bar{R}$ for every valuation ring N in $\mathfrak{V}(R)$, and our theorem will clearly follow if we show that there is then a splitting $F(U)=G(U)H(U)$ in $R[U]$ such that $\bar{G}_N(U) \doteq \Phi_N(U)$ and $\bar{H}_N(U) \doteq \Theta_N(U)$ for every N in $\mathfrak{V}(R)$. Let y be the associated point of Z, and consider the rational transform $y(R)$; since R is a regular local ring of dimension 2, there exists according to Theorem 1, Corollary 1, a finite quadratic transform $z(R)$ of a certain order π

(along a suitable sequence of valuations) such that the correspondence from $z(R)$ to $y(R)$ is everywhere regular. In case $\pi = 0$, i.e., $z(R) = R$, the center $\bar{y}(R)$ is a uniquely determined point and the corresponding form is just the residue form $\bar{F}(U)$; it follows that $\bar{F}_N(U) = \bar{F}(U)$ for every N in $\mathfrak{V}(R)$, so that all forms in the system $\bar{F}_R(U)$ are essentially the same. Now, there are only a finite number of ways in which the form $\bar{F}(U)$ can split into two factors and the set of all N such that the splitting $\bar{F}_N(U) = \Phi_N(U)\Theta_N(U)$ coincides with a given splitting of $\bar{F}(U)$ is easily seen to be a closed subset in $\mathfrak{V}(R)$. Since according to Theorem 1, Corollary 2, the space $\mathfrak{V}(R)$ is connected, it follows that all splittings in the given $\bar{R}$-disjoint splitting of the system $\bar{F}_R(U)$ must coincide with one single splitting $\bar{F}(U) \doteq \Phi(U)\Theta(U)$; furthermore, since $\bar{F}(U)$ is rational over $\bar{R}$ and the splitting is $\bar{R}$-disjoint, it follows that both $\Phi(U)$ and $\Theta(U)$ must be rational over $\bar{R}$. By Hensel's Lemma for the local ring R, there exist forms $G(U)$ and $H(U)$ in $R[U]$ such that $F(U) = G(U)H(U)$, $\bar{G}(U) \doteq \Phi(U)$, and $\bar{H}(U) \doteq \Theta(U)$. This proves our assertion for $\pi = 0$. We shall prove our assertion in the general case by induction on the order π of $z(R)$; we therefore assume that our assertion has already been proved for the case where $y(R)$ is an everywhere regular transform of a finite quadratic transform of R of order less than π.

It is well-known that R is a unique -factorization ring; for convenience, we shall assume that the coefficients in $F(U)$ have been so chosen that they are all in R, but without any common factor. Consider the homogeneous residue form $\boldsymbol{F}(U)$ of $F(U)$; since $\boldsymbol{F}(U)$ differs from $\bar{F}_M(U)$ only by a proportionality factor in $\bar{R}(\boldsymbol{x})$ (we recall that $M = Q(x(\mathrm{R})/\zeta)$ and ζ is the point in $\bar{x}(R)$ with $(\boldsymbol{x}_1, \cdots, \boldsymbol{x}_t)$ as homogeneous coordinates), the given splitting $\bar{F}_M(U) \doteq \Phi_M(U)\Theta_M(U)$ induces a splitting $\boldsymbol{F}(U) \doteq \Phi(U)\Theta(U)$ in $\bar{R}[\boldsymbol{x}]$, with $\Phi(U) \doteq \Phi_M(U)$ and $\Theta(U) \doteq \Theta_M(U)$. We assume now that (A) *the leading coefficient α in $\boldsymbol{F}(U)$ does not vanish*; if we denote by δ the highest common factor (in $\bar{R}[\boldsymbol{x}]$) of all coefficients in $\boldsymbol{F}(U)$, and choose the forms $\Phi(U)$ and $\Theta(U)$ (which are each determined up to a proportionality factor in $\bar{R}(\boldsymbol{x})$) so that the coefficients of each form are all in $\bar{R}[\boldsymbol{x}]$ but without any common factor, then we have $\boldsymbol{F}(U) = \delta\Phi(U)\Theta(U)$ up to a proportionality factor in $\bar{R}$, which can be absorbed in δ. If β and γ are the leading coefficients in $\Phi(U)$ and $\Theta(U)$ respectively, we have then $\alpha = \delta\beta\gamma$; we assume that (B) *the elements δ, β, γ are relatively prime.* The properties (A) and (B) assumed here, if not already present, can be easily obtained as follows. Let $w = (w_0, w_1, \cdots, w_n)$ be a system of independent variables over K, and consider the complete local ring $R(w)^*$, which is also regular and has the dimension 2, attached to Λ by identifying the elements $\bar{w} = (\bar{w}_0, \bar{w}_1, \cdots, w_n)$ as a system of independent variables over $\bar{R}$. We apply to $F(U)$ the linear

transformation which leaves $U_1, \cdots, U_n$ invariant but carries U_0 into $\sum_{i=0}^{n} w_i U_i$ and apply to $\boldsymbol{F}(U)$, $\Phi(U)$, $\Theta(U)$ the corresponding transformation whereby $U_1, \cdots, U_n$ remain invariant but U_0 is carried into $\sum_{i=0}^{n} \bar{w}_i U_i$; then the elements $\boldsymbol{F}(\bar{w})$, $\Phi(\bar{w})$, and $\Theta(\bar{w})$ becomes the leading coefficients of the transformed forms of $\boldsymbol{F}(U)$, $\Phi(U)$, and $\Theta(U)$ respectively. It is clear that our problem is invariant under such a linear transformation. Now, it is obvious that (A) holds for the transformed forms; while as to (B), we need only to observe that any common factor (in $\bar{R}[\boldsymbol{x}]$) of all coefficients in $\boldsymbol{F}(U)$ appears with the minimum power in $\boldsymbol{F}(\bar{w})$ (so that we can assume δ to be relatively prime to β and γ), and that since $\Phi(U)$ and $\Theta(U)$ are relatively prime with their coefficients determined as indicated above, the elements $\Phi(\bar{w})$ and $\Theta(\bar{w})$ must be relatively prime (so that we can assume β and γ to be relatively prime). On the other hand, since the field K is algebraically closed in the quotient field of $R(w)^*$, any splitting $F(U) = G(U)H(U)$ of $F(U)$ in $R(w)^*[U]$ must be already a splitting in $R[U]$, so that the validity of our assertion for $R(w)^*$ will imply its validity for R. Thus we have shown that we can assume the properties (A) and (B) without any loss of generality.

Let λ be the order of $F(U)$ in its power series development as a form in $M^*[U]$, and let a be the leading coefficient $F(U)$; by (A), the order of a must also be λ and we have $\boldsymbol{a} = \alpha = \beta\gamma\delta$, so that λ is also the degree of α (as a form in $\bar{R}[\boldsymbol{x}]$). Let μ, ν, ϵ be the degrees of β, γ, δ respectively, so that $\lambda = \mu + \nu + \epsilon$.

We now invoke a property of the local ring R which is dependent on its dimension being 2. According to [8], Satz 9 (see item (b) in the proof), any splitting of $\boldsymbol{a}$ into relatively prime elements is induced by a corresponding splitting of a in R. Since β, γ, δ are relatively prime, there exist therefore elements b, c, d in R such that $a = bcd$, $\boldsymbol{b} = \beta$, $\boldsymbol{c} = \gamma$, $\boldsymbol{d} = \delta$. Let $\delta = \delta_1 \cdots \delta_s$ be the factorization of δ into powers of distinct prime elements in $\bar{R}[\boldsymbol{x}]$; there exist then elements $d_1, \cdots, d_s$ in R such that $d = d_1 \cdots d_s$, $\boldsymbol{d}_1 = \delta_1, \cdots$ $\boldsymbol{d}_s = \delta_s$. We denote by ϵ_i the order of d_i, which is the degree of δ_i, so that $\epsilon = \epsilon_1 + \cdots + \epsilon_s$. We observe that since each δ_i is a power of an irreducible form in $\bar{R}[\boldsymbol{x}]$, it determines a point $\xi^{(i)}$ in $\bar{x}(R)$, unique up to conjugates over $\bar{R}$, which is algebraic over $\bar{R}$, so that $Q(x(R)/\xi^{(i)})$ has the dimension 2.

Let η be a point in $\bar{x}(R)$; following the notations introduced in the proof of Lemma 5.1, we shall denote the completion of $Q(x(R)/\eta)$ by R_1, and we observe that R_1 is now a complete regular local ring of dimension $\leqq$ 2 (the dimension is equal to 1 if and only if η is a generic point of $\bar{x}(R)$ over $\bar{R}$). Let $z'(R_1)$ be the finite quadratic transform of R_1 along the subseque

those valuations in the definition of $z(R)$ which dominate $Q(x(R)/\eta)$, or rather the sequence of the extensions of these (real discrete) valuations to R_1; it is easily seen that the correspondence from $z'(R_1)$ to $z(R_1)$ is regular everywhere, from which it follows that the correspondence from $z'(R_1)$ to $y(R_1)$ is also regular everywhere. Since the order of the quadratic transform $z'(R_1)$ is evidently less than π, we can apply our induction hypothesis. We recall that if N is any valuation ring dominating R, then by definition $\Phi_N(U) = \Phi_{K\cap N}(U)$ and $\Theta_N(U) = \Theta_{K\cap N}(U)$, and that $\Phi_{R_1}(U)$ and $\Theta_{R_1}(U)$ are subsystems of $\Phi_R(U)$ and $\Theta_R(U)$ respectively obtained by restricting N to valution rings dominating R_1. It is clear that the equation $\bar{F}_N(U) = \Phi_N(U)\Theta_N(U)$, for every N dominating R_1, defines a splitting of $\bar{F}_{R_1}(U)$ into the two systems $\Phi_{R_1}(U)$ and $\Theta_{R_1}(U)$, which is clearly $\bar{R}$-disjoint and hence also $\bar{R}(\eta)$-disjoint. By induction hypothesis, there exists therefore a splitting $F(U) = G_\eta(U)H_\eta(U)$ in $R_1[U]$ such that $G_\eta(U)$ generates the system $\Phi_{R_1}(U)$ and $H_\eta(U)$ generates the system $\Theta_{R_1}(U)$. Now, this splitting $F(U) = G_\eta(U)H_\eta(U)$ in $R_1[U]$ implies a splitting of the leading coefficient a in $F(U)$ into two factors in R_1, which we shall now proceed to investigate. Without any loss of generality, we can assume for convenience that $\eta_1 \neq 0$, as we did in the proof of Lemma 5.1; then all coefficients in $F(U)$ are divisible by $x_1{}^\lambda$ in R_1, and since R_1 is a unique factorization ring, there exist positive integers λ' and λ'' ($\lambda' + \lambda'' = \lambda$) such that all coefficients in $G_\eta(U)$ are divisible by $x_1{}^{\lambda'}$ and all coefficients in $H_\eta(U)$ are divisible by $x_1{}^{\lambda''}$. If we set $F^0(U) = (1/x_1)^\lambda F(U)$, $G^0(U) = (1/x_1)^{\lambda'}G_\eta(U)$, and $H^0(U) = (1/x_1)^{\lambda''}H_\eta(U)$, then we have evidently the splitting $F^0(U) = G^0(U)H^0(U)$ in $R_1[U]$. We set $a^0 = (1/x_1)^\lambda a$, $b^0 = (1/x_1)^\mu b$, $c^0 = (1/x_1)^\nu c$, $d^0 = (1/x_1)^\epsilon d$, and $d_i{}^0 = (1/x_1)^{\epsilon_i} d_i$; then the elements a^0, b^0, c^0, d^0, $d_i{}^0$ are all in R_1, and a^0 is the leading coefficient in $F^0(U)$. The situation divides into two cases, which we shall treat separately.

(1) The point η coincides with one of the points $\xi^{(1)}, \cdots, \xi^{(s)}$, say $\xi^{(j)}$. In this case, it is easily seen that the elements b^0, c^0, $d_i{}^0$ $(i \neq j)$ are all units in R_1; for example, the p_1-residue of b^0 is the value of β for $\boldsymbol{x}_1 = 1$, $\boldsymbol{x}_2 = \eta_2/\eta_1$, which is not zero since β and δ_j are relatively prime in $\bar{R}[\boldsymbol{x}]$. The splitting $F^0(U) = G^0(U)H^0(U)$ induces therefore a splitting of $d_j{}^0$ into two factors in R_1. We maintain that this splitting of $d_j{}^0$ is induced by a splitting $d_j = d'_j d''_j$ in R; in other words, if ϵ' and ϵ'' are the orders of d'_j and d''_j respectively, then the given splitting of $d_j{}^0$ coincides with the splitting $d_j{}^0 = (d'_j/x_1{}^{\epsilon'})(d''_j/x_1{}^{\epsilon''})$ up to units in R_1. To prove this, it is sufficient to show that if e is a prime factor of d_j, of order ρ in M, then $e^0 = e/x_1{}^\rho$ must with prime element in R_1; for we can then apply this argument to every

prime factor of d_j and obtain a complete factorization of $d_j{}^0$ in R_1, and our assertion then follows from the unique factorization property of R_1. First, we note that e^0 is a prime element in $R[x_2/x_1]$; for, if e^0 splits into two factors in $R[x_2/x_1]$, they must be of the form $e'/x_1{}^{\rho'}$ and $e''/x_1{}^{\rho''}$ with e' and e'' in R, and again the unique factorization property in R shows that we must have $\rho = \rho' + \rho''$ and hence $e = e'e''$. Next, since $\mathfrak{Q}(x(R)/\eta)$ is the quotient ring of $R[x_2/x_1]$ with respect to a prime ideal which contains the element e^0, it follows from a well-known property of quotient ring that e^0 must remain a prime element in $Q(x(R)/\eta)$. Now, consider the residue rings R/Re and $Q(x(R)/\eta)/Q(x(R)/\eta)e^0$; since $Q(x(R)/\eta)e^0 \cap R = R[x_2/x_1]e^0 \cap R = Re$, we can embed the former canonically in the latter. It is clear that both rings are local domains of dimension 1, and that their residue fields can be identified with $\bar{R}$ and $\bar{R}(\eta)$ respectively. Since R is complete, R/Re is also complete, and since $\bar{R}(\eta)$ is algebraic over $\bar{R}$, it follows ([6], Theorem 8) that $Q(x(R)/\eta)/Q(x(R)/\eta)e^0$ is a finite module over R/Re and hence ([3], § III, Proposition 8) must also be complete. This implies that

$$Q(x(R)/\eta)/Q(x(R)/\eta)e^0 = R_1/R_1e^0,$$

so that R_1/R_1e^0 is a local domain; this shows that e^0 is a prime element in R_1. It is clear that since $d'_j/x_1{}^{\epsilon'}$ and $d''_j/x_1{}^{\epsilon''}$ coincide up to units in R_1 with the leading coefficients in $G^0(U)$ and $H^0(U)$ respectively, we can take as the respective leading coefficients in the forms $G_\eta(U)$ and $H_\eta(U)$ any multiples of d'_j and d''_j in R which are factors in a splitting of a in R.

(2) The point η is distinct from the points $\xi^{(1)}, \cdots, \xi^{(s)}$. In this case, the form $\boldsymbol{F}(U)$ does not vanish identically at the point η, and hence at least one coefficient in $F^0(U)$ must be a unit in R_1; and this implies that also both $G^0(U)$ and $H^0(U)$ must have at least one coefficient which is a unit in R_1. If we denote by $\bar{F}^0(U)$, $\bar{G}^0(U)$, and $\bar{H}^0(U)$ the respective residue forms in $\bar{R}_1[U]$, then we must have $F^0{}_N(U) \doteq \bar{F}^0(U)$, $G^0{}_N(U) \doteq \bar{G}^0(U)$, and $H^0{}_N(U) \doteq \bar{H}^0(U)$ for every valuation ring N dominating R_1; it follows that $\Phi_N(U) \doteq \bar{G}^0(U)$ and $\Theta_N(U) \doteq \bar{H}^0(U)$ for every N dominating R_1, and hence in particular $\Phi_{M_1}(U) \doteq \bar{G}^0(U)$ and $\Theta_{M_1}(U) \doteq \bar{H}^0(U)$, where M_1 is the valuation ring of rank 2 introduced after Lemma 5.1. On the other hand, since M'^* is a quotient ring of M_1, $\Phi_{M_1}(U)$ and $\Theta_{M_1}(U)$ are specializations of $\Theta_{M'^*}(U) = \Phi_M(U)$ and $\Phi_{M'^*}(U) = \Theta_M(U)$ respectively over the specialization $\zeta \to \eta$ over $\bar{R}$; it follows that $\bar{G}^0(U)$ and $\bar{H}^0(U)$ are up to proportionality factors equal to the forms obtained from $\Phi(U)$ and $\Theta(U)$ respectively by setting $(\boldsymbol{x}_1, \boldsymbol{x}_2) = (\eta_1, \eta_2)$. Now, since β and γ have no common factor in $\bar{R}[\boldsymbol{x}]$, at least one of them does not vanish at the point η. If β does not vanish at η, then the leading coefficient in $\bar{G}^0(U)$ does not vanish and hence

he leading coefficient in $G^0(U)$ must be a unit in R_1; since in this case the lements b and d^0 are units in R_1, the leading coefficient in $H^0(U)$ must be qual to c up to a unit in R_1. On the other hand, if γ does not vanish at η, hen the same argument with $G^0(U)$ and $H^0(U)$ interchanged, shows that ^{0} and d^0 are units in R_1, and that the leading coefficient in $G^0(U)$ must be qual to b up to a unit in R_1. Going over to the forms $G_\eta(U)$ and $H_\eta(U)$, re conclude that wec an take as their respective leading coefficients any aultiples of b and c in R which are factors in a splitting of a in R.

We set $d' = d'_1 \cdot \cdot \cdot d'_s$ and $d'' = d''_1 \cdot \cdot \cdot d''_s$, so that we have $d = d'd''$, nd consider the splitting $a = bd' \cdot cd''$ in R. We shall now normalize the orms $G_\eta(U)$ and $H_\eta(U)$, for every point η in $\bar{x}(R)$, by taking bd' as the eading coefficient in $G_\eta(U)$ and cd'' as the leading coefficient in $H_\eta(U)$. 'his choice of the leading coefficients is permissible in view of what we have ust shown above. For $\eta = \zeta$, we obtain a splitting $F(U) = G_\zeta(U)H_\zeta(U)$ a $M^*[U]$; incidentally, we observe that this is the splitting according to Iensel's Lemma with the intial conditions $(\Phi_M(U), \Theta_M(U); bd', cd'')$, in the erminology introduced at the end of the section 4. We shall now show that $G_\zeta(U) = G_\eta(U)$ and $H_\zeta(U) = H_\eta(U)$ for every point η in $\bar{x}(R)$, in the ense that they are the same forms in $M'^*[U]$, so that all the splittings $F(U) = G_\eta(U)H_\eta(U)$ are in reality one and the same. This will prove our heorem. For, then the forms $G_\zeta(U)$ and $H_\zeta(U)$ must be both in $R[U]$ ccording to Lemma 5.1 (applied to every coefficient in them); if we set $G(U) = G_\zeta(U)$ and $H(U) = H_\zeta(U)$, then $F(U) = G(U)H(U)$ is a splitting n $R[U]$ and it is clear that $\bar{G}_N(U) \doteq \Phi_N(U)$ and $\bar{H}_N(U) \doteq \Phi_N(U)$ for every valuation ring N in K dominating R.

It remains therefore to show that $G_\zeta(U) = G_\eta(U)$ and $H_\zeta(U) = H_\eta(U)$, or every point η in $\bar{x}(R)$, whereby we shall use again the notations introduced n the proof of Lemma 5.1. Consider the valuation ring M_1 of rank 2 ntroduced after Lemma 5.1. It is clear that

$$\bar{G}_{\zeta,M'^*}(U) \doteq \bar{G}_{\zeta,M}(U) \doteq \Phi_M(U) \doteq \Phi_{M'^*}(U)$$

ınd

$$\bar{H}_{\zeta,M'^*}(U) \doteq \bar{H}_{\zeta,M}(U) \doteq \Theta_M(U) \doteq \Theta_{M'^*}(U);$$

ince M'^* is a quotient ring of M_1, it follows that both $\bar{G}_{\zeta,M_1}(U)$ and $\Phi_{M_1}(U)$ ıre specializations of $\Phi_M(U)$ over the specialization $\zeta \rightarrow \eta$ over $\bar{R}$, and that oth $\bar{H}_{\zeta,M_1}(U)$ and $\Theta_{M_1}(U)$ are specializations of $\Theta_M(U)$ over the specialization $\zeta \rightarrow \eta$ over $\bar{R}$. Since $\bar{x}(R)$ is a non-singular curve, the specializations of oth $\Phi_M(U)$ and $\Theta_M(U)$ over the specialization $\zeta \rightarrow \eta$ over $\bar{R}$ must be unique; t follows that $\bar{G}_{\zeta,M_1}(U) \doteq \Phi_{M_1}(U)$ and $\bar{H}_{\zeta,M_1}(U) \doteq \Theta_{M_1}(U)$. On the other hand, by the inductive hypothesis, we have $\bar{G}_{\eta,M_1}(U) \doteq \Phi_{M_1}(U)$ and $\bar{H}_{\eta,M_1}(U)$

$\doteq \mathfrak{G}_{M_1}(U)$. This shows that $\bar{G}_{\zeta,M_1}(U) \doteq \bar{G}_{\eta,M_1}(U)$ and $\bar{H}_{\zeta,M_1}(U) \doteq \bar{H}_{\eta,M_1}(U)$. Recalling that the forms $G_\zeta(U)$ and $G_\eta(U)$ have the same leading coefficient bd', and that the forms $H_\zeta(U)$ and $H_\eta(U)$ have the same leading coefficient cd'', we see that the two splittings $F(U) = G_\zeta(U)H_\zeta(U)$ and $F(U) = G_\eta(U)H_\eta(U)$ in $M_1[U]$ have the same initial condition

$$(\bar{G}_{\zeta,M_1}(U), \bar{H}_{\zeta,M_1}(U); bd', cd'') = (\bar{G}_{\eta,M_1}(U), \bar{H}_{\eta,M_1}(U); bd', cd'');$$

it follows from the remark at the end of section 4 that $G_\zeta(U) = G_\eta(U)$ and $H_\zeta(U) = H_\eta(U)$. This concludes the proof of Theorem 2.

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] Abhyankar, S., and Zariski, O., "Splitting of valuations in extensions of local domains. I," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 84-90.

[2] Abhyankar, S., "On the valuations centered in a local domain," *American Journal of Mathematics*, vol. 78 (1956), pp. 321-48.

[3] Chevalley, C., "On the theory of local rings," *Annals of Mathematics*, vol. 44 (1943), pp. 690-708.

[4] Chow, W. L., "On the principle of degeneration in algebraic geometry," *Annals of Mathematics*, vol. 66 (1957), pp. 70-79.

[5] ———, "On the theorem of Bertini for local domains," *Proceedings of the National Academy of Sciences*, vol. 44 (1958), pp. 580-584.

[6] Cohen, I. S., "On the structure and ideal theory of complete local rings," *Transactions of the American Mathematical Society*, vol. 59 (1946), pp. 54-106.

[7] Krull, W., "Ein Satz ueber primaere Integritaetsbereiche," *Mathematische Annalen*, vol. 103 (1930), pp. 450-465.

[8] ———, "Zur Theorie der kommutativen Integritaetsbereiche," *Journal fuer die reine und angewandte Mathematik*, vol. 192 (1954), pp. 230-252.

[9] Murre, J. P., "On a connectedness theorem for a birational transformation at a simple point," *American Journal of Mathematics*, vol. 80 (1958), pp. 3-15.

[10] Nagata, M., "Note on a chain condition for prime ideals," *Memoirs of the College of Science, University of Kyoto*, Series A, vol. 32 (1959), pp. 85-90.

[11] Zariski, O., "Foundations of a general theory of birational correspondences," *Transactions of the American Mathematical Society*, vol. 53 (1943), pp. 490-542.

[12] ———, "Analytical irreducibility of normal varieties," *Annals of Mathematics*, vol. 49 (1948), pp. 352-361.

[13] ———, "A simple analytical proof of the fundamental property of birational transformations," *Proceedings of the National Academy of Sciences*, vol. 35 (1949), pp. 62-66.

[14] ———, "Theory and applications of holomorphic functions on algebraic varieties over arbitrary ground fields," *Memoirs of the American Mathematical Society*, No. 5, 1951.

[15] ———, "The connectedness theorem for birational transformations," *Algebraic Geometry and Topology*, A symposium in honor of S. Lefschetz, Princeton, 1957, pp. 182-188.